

Trisul Network Metering and Forensics

Really know your network

(c) Unleash Networks 2009, All rights reserved



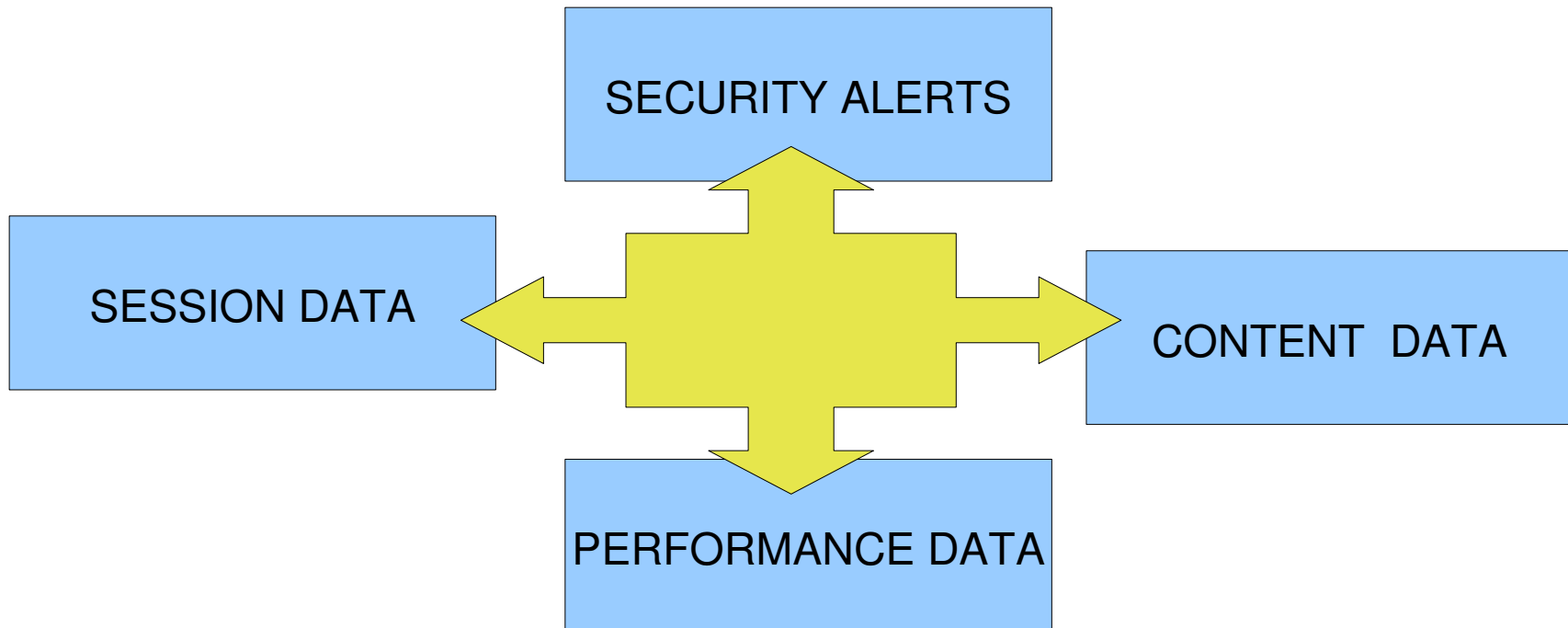
Trisul Network Metering and Forensics



What is Trisul

TRISUL

- A new Network Security Monitoring platform
- Gives you unprecedented visibility into your network activity
- Real time and Retro analysis features
- Pulls together four vital aspects of today's networks



Trisul Network Metering and Forensics



Trisul capabilities

- 24x7 Linux based
- Runs on commodity hardware
- Supports Packet capture, Netflow, or PCAP import
- Tracks detailed L2 and L3 usage statistics
- Isolate and drilldown specific targets
- Stores raw packets for deep inspection (forensics)
- Stores flow details
- Integrated with Snort IDS to correlates threats
- Support for various top-N

How it differs from SNMP and Netflow based tools ?

- Can track Layer 2 events and anomalies
- Gives you exact packets that can later be investigated by Unsniff or Wireshark
- Jump from statistics to flows to security alerts – finally to raw content
- Much more granular than Netflow, no load on router if using a tap
- Trisul can also accept Netflow records (so it is a superset of Netflow based tools)

Trisul Network Metering and Forensics



Applications

- 24X7 perimeter monitoring
- Pin point network utilization tracking
- Data Leak Prevention
- Aid incident investigation
- Retro analysis help desk
- Track down L2 issues now and in the past
- Policy violations
- Statutory monitoring as part of SLA
- Part of corporate security posture
- Daily security and health reporting via PDF reports
- more..

Trisul Network Metering and Forensics



Security Features

Due to the sensitive nature of the product it has been designed with security in mind

- Forensics Module is optional
- Multiple layers of security
- All communication over TLS (DHE is the default key exchange)
- ACL only allows certain subnets to access the system
- Three levels of access (Admin, Operator, Forensics)
- Each user requires current certificate from network administrator
- If forensics enabled, content further encrypted by AES-128
- Can filter privileged subnets/hosts from being monitored

Trisul Network Metering and Forensics

Products in the Trisul family



Trisul Network Metering and Forensics
Core 24x7 platform



Unsniff Network Analyzer 2.0
Portable network analysis platform. Windows based multi layer visualizer for Trisul



Web Trisul
Web based interface to Trisul. Available in Beta today and GA in Dec 09.



Trisul Network Metering and Forensics

Who we are

- Unleash Networks
- Technology partner of Elina Networks
- Deep knowledge of Mobile and IP Core technologies
- Make cutting edge products for network analysis
- Deep packet inspection, security, and forensics a key strength
- Awarded Nasscom Top 100 Innovators of 2007

Flexible Plans

- Deployment of 24x7 monitoring platform Trisul
- IP / GPRS Packet Core Network Auditing
- Month-to-month rental based deployment also available
- IP Security monitoring and auditing also available
- Other time limited services



Trisul Network Metering and Forensics

You can download time limited versions of some of our software

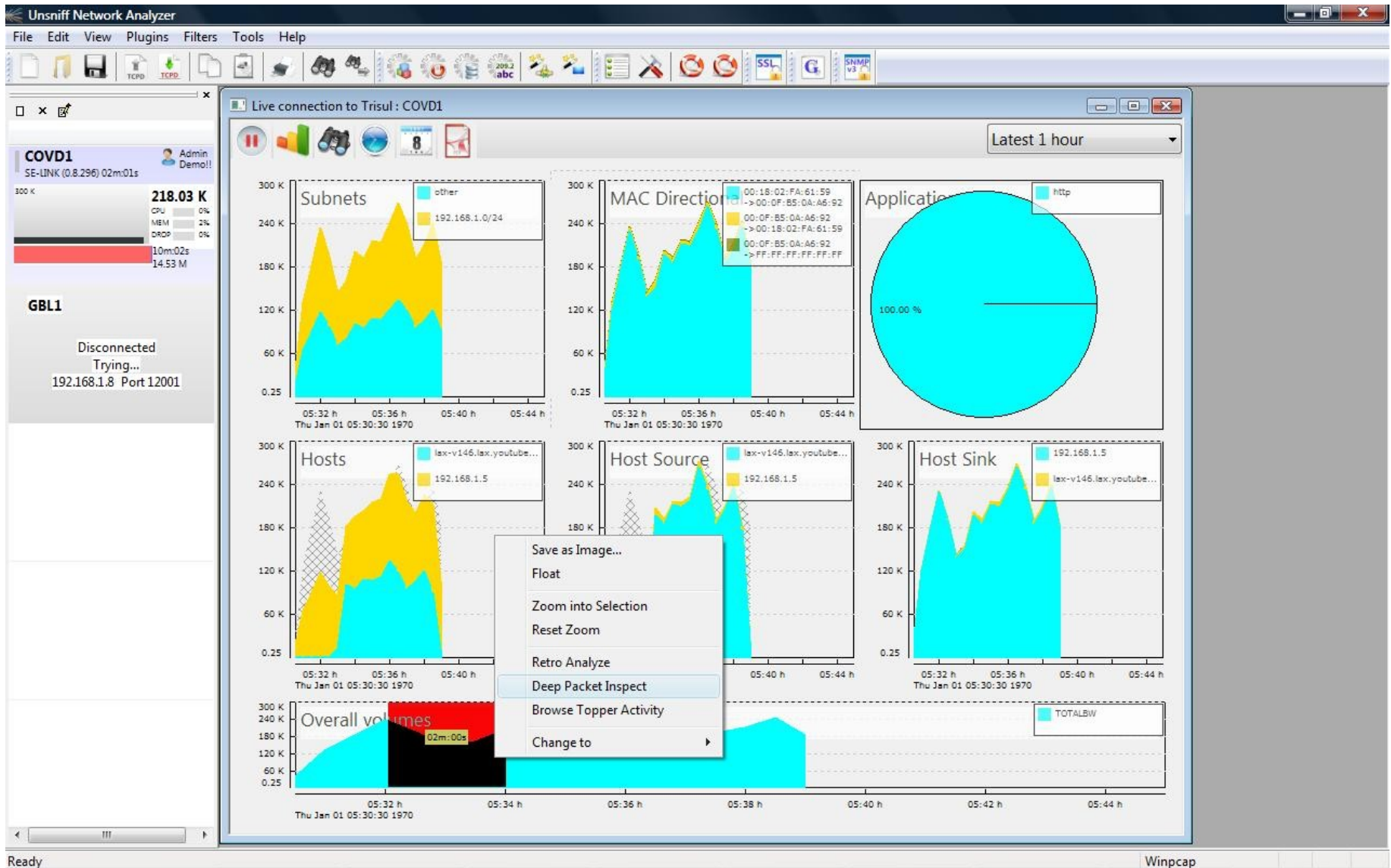
<http://www.unleashnetworks.com>

THANK YOU



Trisul Network Metering and Forensics

Live view and drilldown



Trisul Network Metering and Forensics

Flow monitoring

The screenshot displays the Unsniff Network Analyzer interface. The main window is titled "Tracking flows [Highest volume] at Trisul COVID1" and shows a table of network flows. The table has columns for R (Remote), Address, Port, Address, Port, Forward Bytes, Reverse Bytes, Started, and D (Destination). The data shows various flows, including a large one to lax-v146.lax.youtube.com and several to 192.168.1.5.

R	Address	Port	Address	Port	Forward Bytes	Reverse Bytes	Started	D
1	lax-v146.lax.youtube.com	http	192.168.1.5	Port-4395	9.87 M	231.39 K	Thu Jan 01 05:33:53 1970 714954	0
2	192.168.1.5	Port-4375	v102.youtube.com	http	81.12 K	3.38 M	Thu Jan 01 05:31:09 1970 482396	0
3	192.168.1.5	Port-4373	216.239.51.176	http	24.31 K	95.28 K	Thu Jan 01 05:30:52 1970 688048	3
4	192.168.1.5	Port-4372	216.239.51.176	http	16.86 K	67.67 K	Thu Jan 01 05:30:52 1970 679845	3
5	192.168.1.5	Port-4389	208.65.153.253	http	3.95 K	54.17 K	Thu Jan 01 05:33:45 1970 338579	0
6	192.168.1.5	Port-4366	208.65.153.253	http	5.56 K	44.80 K	Thu Jan 01 05:30:46 1970 841075	2
7	192.168.1.5	Port-4394	216.239.51.176	http	6.85 K	29.79 K	Thu Jan 01 05:33:48 1970 578325	1
8	192.168.1.5	ds-admin	216.239.51.176	http	6.63 K	26.09 K	Thu Jan 01 05:36:17 1970 877482	1
9	192.168.1.5	ds-user	216.239.51.176	http	6.47 K	22.41 K	Thu Jan 01 05:36:17 1970 869153	1
10	80.67.87.41	http	192.168.1.5	Port-4392	24.47 K	1.18 K	Thu Jan 01 05:33:48 1970 373153	0
11	192.168.1.5	Port-4367	208.65.153.253	http	5.20 K	19.37 K	Thu Jan 01 05:30:48 1970 242293	2
12	192.168.1.5	Port-4393	216.239.51.176	http	4.09 K	16.99 K	Thu Jan 01 05:33:48 1970 570398	1
13	192.168.1.5	Port-4382	208.65.153.253	http	2.55 K	11.48 K	Thu Jan 01 05:33:25 1970 339200	0
14	192.168.1.5	epmd	209.85.143.166	http	3.04 K	10.48 K	Thu Jan 01 05:30:48 1970 962081	0
15	192.168.1.5	Port-4387	209.85.143.166	http	1.78 K	9.93 K	Thu Jan 01 05:33:31 1970 029437	0

On the left side, there is a summary for "COVID1" showing a total of 218.03 K bytes. Below that, a status for "GBL1" is shown as "Disconnected Trying..." with the IP address 192.168.1.8 and Port 12001.

At the bottom of the window, a status bar indicates "Opening secure connection to TRISUL : COVID1 ..." and "Winpcap".