Clusterpoint Network Traffic Surveillance System

Data Sheet

"Protecting information is critical for any organization since the consequences of unauthorized disclosure can spell lost customers, irreparable brand damage, or potential liability … "

Chris Leach Keynote speaker for IDC's Fifth Annual Security Summit.

Do you want to get relevant information on your network traffic content less than in a second?

Turn-key Enterprise Internet Security Solution

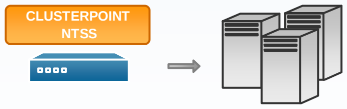
Clusterpoint Network Traffic Surveillance System (NTSS) is an Internet data traffic recording and archiving system, which captures IP packets from an Ethernet network, re-engineers relevant traffic back to the application level content (Web pages, e-mails, downloaded and uploaded files etc.) and stores it into the Clusterpoint scalable and searchable database system for long term archiving and records management needs.

In essence, NTSS operates similarly to the video surveillance systems commonly used for monitoring of people movements into/out of the building. Yet NTSS is radically different and much more powerful tool.

How does it work?

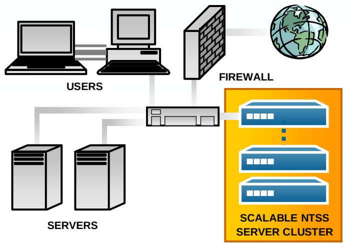
Step 1

Unpack and connect to the corporate network



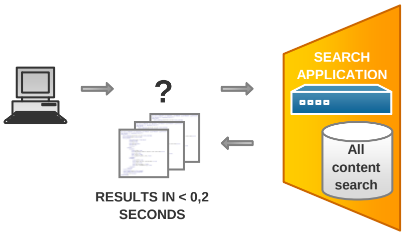
Step 2

Let the NTSS capture, analyze and store traffic flows



Step 3

Search through the stored information by content, user, date and time or any other parameter



The Scope of uses

Unlike video surveillance systems providing just camera recordings and their playback for specific time frames, NTSS system can retrieve any suspicious traffic by any content or parameters within IP packets it has captured. In this way it is possible to ask the system queries, for example:

- who posted a comment with known keywords on an Internet portal some months ago;
- who sent or received emails with some attachments or texts which could indicate fraud or other dishonest activities etc.

New Technology

Clusterpoint NTSS is built on the innovative, totally searchable and scalable Clusterpoint Database Management System (DBMS) that can store any data in XML format.
All the data stored are indexed for full content access. This database technology allows to store large amounts data captured by the NTSS in a cost effective manner and provide full text and structured search results from those data in sub-second times.
In case of upgrades, every next appliance plugs into the network to operate as a distributed system that shares the workload of processing data, and increases the storage size for the collected data.
No need for box replacement when undertaking capacity upgrades or expansion.

System Architecture

NTSS consists of following components:
Traffic capturing and recording module

- It captures and records all specified network traffic flows at IP level and aggregated documents level;
- Re-engineers from all TCP/IP packets relevant traffic protocols back into the application level data (Web pages, emails, attachment files, file downloads, chat messages etc.) and indexes it for instant search;
- Supports transparent bridge mode for undetectable traffic monitoring and recording on the network.

Clusterpoint Server

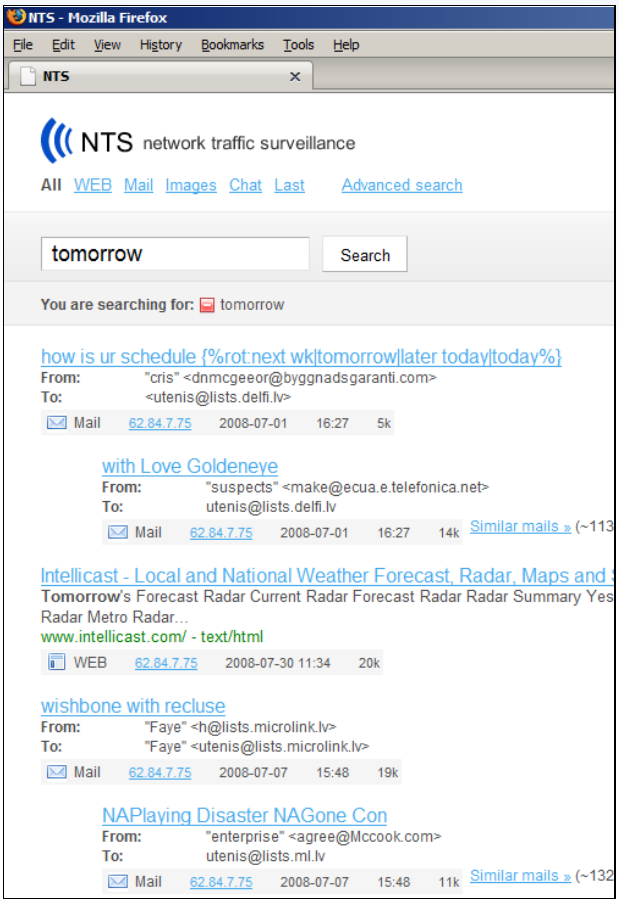
- provides system totally scalable cluster architecture to accommodate growing traffic database at fixed price per gigabyte;
- provides advanced multi-language full content search

Clusterpoint Network Traffic Surveillance System

Data Sheet

Appliance

- 1U rack mountable HP Proliant DL360G5 server appliance with Quad-Core Intel® Xeon® Processor, 4GB RAM;
- Two Integrated PCI Express Gigabit Server Adapters;
- Pre-installed Clusterpoint NTSS software package;
- Access through WEB interface.


NTS - Mozilla Firefox
File Edit View History Bookmarks Tools Help
NTS
NTS network traffic surveillance
All WEB Mail Images Chat Last Advanced search
tomorrow
Search

You are searching for: tomorrow

how is ur schedule {%rot:next wk|tomorrow|later today|today%}
From: "cris" <dnmcgeeor@byggnadsgaranti.com>
To: <utenis@lists.delfi.lv>
Mail 62.84.7.75 2008-07-01 16:27 5k

with Love Goldeneye
From: "suspects" <make@ecua.e.telefonica.net>
To: utenis@lists.delfi.lv
Mail 62.84.7.75 2008-07-01 16:27 14k Similar mails » (~113

Intellicast - Local and National Weather Forecast, Radar, Maps and
Tomorrow's Forecast Radar Current Radar Forecast Radar Radar Summary Yes
Radar Metro Radar...
www.intellicast.com/ - text/html
WEB 62.84.7.75 2008-07-30 11:34 20k

wishbone with recluse
From: "Faye" <h@lists.microlink.lv>
To: "Faye" <utenis@lists.microlink.lv>
Mail 62.84.7.75 2008-07-07 15:48 19k

NAPlaying Disaster NAGone Con
From: "enterprise" <agree@Mccook.com>
To: utenis@lists.ml.lv
Mail 62.84.7.75 2008-07-07 15:48 11k Similar mails » (~132

Search interface example

Performance built into the Design

The core software for NTSS and the Clusterpoint Server has been developed in C/C++ for the best performance on contemporary commodity hardware systems.
The application itself runs on FreeBSD, however all common management and configuration functions have been implemented in the Manager Application that can be accessed using a simple WEB browser interface.

Information Capture and Storage Features

- NTSS can record all specified network traffic flows;
- It analyses and re-engineers the following protocols:
  - TCP - shows chosen TCP connection data in text or hex formats;
  - HTTP - shows Web pages accessed by users, with all of their content and exactly the same visual way when the user accessed them and maintains database of stored URLs for Web traffic;
  - HTTP POST/GET - information that users wrote into Web forms or posted over the internet;
  - SMTP and POP3 - shows incoming and outgoing emails with all attachments;
  - exact recorded data flow can be specified by IP addresses and ports;
- Centralized system management using WEB interface;
- Tools for performance tuning;
- User security and group security based administration tool;
- VIP addresses – specify IP addresses or subnets that will not be monitored;
- NTSS can be plugged into existing computer network as a transparent bridge, or connected to a specific computer/server. It can be as well connected to a specific part of a computer network, or the common Internet gateway segment to capture and record all traffic;
- NTSS can be connected to the monitoring (broadcasting) port of Ethernet switch;
- It is totally undetectable to the users of the computer network (does not show IP address on the network, does not require network configuration changes).
- Multiple languages content - all data are stored as UTF-8.

Information Search and Monitoring Features

- Simple or Advanced search interface options;
- Search filtering:
  - by content type,
  - by IP address,
  - by Date/Time, etc.;
- WEB friendly navigation;
- WEB page previews – view reengineered WEB pages the same way as network users last saw them;
- Highlighted query terms in full text search results;
- Reporting tools.