

Network Forensics is affordable for most Businesses

Forensic systems provide aid in network management

Regulatory requirements such as Sarbanes Oxley or HIPAA along with cyber crime have heightened the interest in computer security. Organizations have started to purchase monitoring systems that not only support network forensics but help organizations understand what information is moving over their key network connections. These frequently are WAN and Internet connections.

Network forensics requires the capture, recording, and analysis of network events. This requires a packet capture tool with analysis capabilities. The Network Analyzer is a perfect backbone for such a system. Most products have strong post capture filtering capabilities and provide network health statistics.

System Requirements

Today's advanced processors and high capacity storage now makes it possible to store large amounts of packet capture data. Although network bandwidth has increased for many homes and small businesses with broadband access, the majority of businesses still rely on T1 connectivity for Internet or WAN connections.

At full utilization a T1 would use approximately 17 gigabytes to record 24 hours of data. But traffic isn't a steady-state phenomenon. It fluctuates a lot and is "bursty." Thus a link can be fully utilized one moment, and then completely empty the next. Also, utilization can be very low during non-business hours. For most companies they can now store better than several weeks of data on a modern system with the addition of a second 300 Gigabyte drive.

For significant bandwidth, such as monitoring Gigabit or Trunked Gigabit requires special considerations. A number of factors come into play. Memory is faster than Disk so Raid Storage can be required; also the utilization of specialized NIC's may be needed to capture the data and buffer what is written to disk.

The products on the market are designed to recycle the storage of data on a first-in first out basis. That way a history is preserved. Some products can monitor a T1 link for as little as \$5,000. There is a great disparity in price, architecture and features. High end pricing for some vendors can approach \$100,000. Appliances may be required on the high end, whereas the low end can be fulfilled with a software solution.

The following table illustrates the storage in Gigabytes needed to provide hours or days of history on heavily utilized WAN connections. It assumes a continuous level of usage 24/7 not likely found in most business networks. You could easily cut the storage requirement down by 1/3 for businesses that run 8:00 to 5:00. You might also be able to cut it again in half, as it is unlikely most businesses are continuously using all of the bandwidth during those office hours. Therefore a 300 Gigabyte drive for many businesses with a T1 connection could easily provide weeks of storage.

Storage Requirements needed for Network Forensics with common WAN Connections

Drive Speed @ 25 Megabytes per Second

Wan Connection	Speed bps	Hours	Gigabytes Storage Required						
			8	16	24	Days	2	4	7
T1	1,544,000		54	108	162		323	646	1131
T3	43,000,000		1499	2999	4498		8996	17992	31486
OC-1	51,850,000		1808	3616	5424		10848	21695	37967
OC-3	155,520,000		5423	10846	16268		32537	65073	113878

* Assumes Full Duplex and 65% continuous utilization. This can be considered a fairly high utilization rate.

** Drives Write Limit bits per second maximum

N/A - Not applicable as it exceeds write capabilities of the drive.

Note: Drive Write Speeds of 15 to 20 MB per second will support all but OC-3

However, it is also interesting to note that the higher bandwidth connections tend to drive the requirement for more sophisticated storage requirements.

Network Forensics

Analysis of the flow of packets over time that network analyzers provide makes it possible to determine when users are active, when they are communicating to other devices, the client-server requests made such as the SQL requests and what Web sites they are visiting.

Traffic analysis can help identify suspect devices. Filter's can be used to identify in the packets a signature of chat sessions, hacks and viruses. Device discovery and switch port discovery can help isolate the devices.

We do not live in a world in which strong encryption is normally placed into the packet payload. Most data flowing across networks or even the internet today is sent without encryption. Many of the tools allow you the ability to reassemble and view/play VOIP, streaming media or even e-mail.

If you are hacked the history can be filtered to try to understand what systems were attacked.

Use of such powerful tools should not be abused. You should have policies on who has access to the system and the circumstances when it should be used along with any restriction on what can be accessed for a given situation. Once the information is accessed policies should specify how to handle or treat the information collected. Companies generally can monitor their own networks, but should notify employees and network users that the monitoring may be taking place by published policies.

Network Analysis

Although Security and Forensics are strong justification for implementation of a continuous packet capture product, other benefits help make for more efficient network operations. Understanding the cause of poor application performance can be just one benefit. But other Network Analysis standards such as Bandwidth Utilization, Protocols and Sub-Protocols in use, level of Broadcasts and Multicasts, Packet Size Distribution and Top Talkers provide valuable information to Network and System Administrators.

Summary

As a result of advancements in processors and storage, it is now possible to keep a history of network activity on key network or WAN segments. The information is not only valuable for Network Forensics but also provides answers to network management and performance questions.

About the Author:

Bruce Warner is the owner of Operative Software Products - www.operativesoft.com. He has over 20 years experience with networking products. Operative Software Products operates in the United States and Canada and provides solutions for test automation, application analysis and network performance.

Copyright 2005