Securing Healthcare Networks Using NetFlow Analyzer - A case study

The Client

A not-for-profit health care system headquartered in California with operations across several states in western United States. This organization comprises of than 85 distinct business units, including 20 hospitals with over 3,100 beds, 18,800 employees, numerous clinics and outpatient facilities, 16 home care agencies and three joint-venture retirement centers.

The Challenge

If their WAN went down for any significant time, it had the potential of costing lives as well as thousands of dollars. So they wanted a system that could provide them with greater control over their network infrastructure. The core requirements were identified to be:

1. Shorten any network downtime by reducing the Mean Time to Repair. They required a system that could produce proactive warnings so that they could address an issue even before the end users were impacted.
2. Ensure optimum performance of their business critical applications by having a visibility into the applications on the network,
3. Identify the top talkers in the network – top hosts and destinations
4. Reduce cost associated with inaccurate bandwidth provisioning

The Solution

ManageEngine NetFlow Analyzer was deployed in this organization to collect and report on NetFlow statistics exported from their Cisco equipment.

Benefits:

ManageEngine NetFlow Analyzer allowed them to perform the following with ease:

1. Knowing what traffic is using what bandwidth on the network which led to reduced time to troubleshoot network down time
2. Track WAN activity by application, and to identify and track virus/worm attacks when they occur.
3. They generate alarms based on thresholds by protocol and when traffic on specific port exceeds a predetermined volume on a specific interface.

4. a) Shorter-duration network incidents, knowing what traffic is using what bandwidth on the network, and better capacity planning all indicate that they are benefiting, mainly from "soft dollar" savings by using NetFlow Analyzer.

   b) Availability of tons of data related to bandwidth consumption made them capable of estimating the kind of bandwidth requirements they had to make provision for accurately. This led to "actual dollar" savings.