Case Study for an IT Services and BPO/KPO company (i7 networks)

Company profile.

- A BPO company providing reliable real estate lease administration related services and onsite support services to customers worldwide.
- Headquartered in US, they run most of their BPO and IT services from India consisting of two units housing about 250+ employees. Yearly revenues more than $100 million.
- Provides project and consulting services, BPO as well as software products for lease and contract abstraction services.

Business situation

The Indian arm of the company does most of the project consulting services, BPO as well as product development activities. The employees are facing network congestion issues leading to reduced productivity and frustration. Controlled internet access, with only a handful of executives exempted from corporate network policies, has helped some but they needed assistance in understanding their network capacity and also to do sizing based on their needs. Increasing bandwidth is an option but they would like to justify the costs with the management for the same with solid data.

Technical situation

The entire Intranet at the Indian branch is under one single subnet. This includes in-house servers and desktop thin clients. Employees are allowed internet access from their thin clients and as well as from their RDP sessions to the servers. Authentication is provided by Microsoft Active Directory. Perimeter security comprises mostly of a mid-range Sonicwall Firewall. Site-to-Site VPN is provided between the HQ and and the Indian branch. Sonicwall Firewall console and reporting tool – ViewPoint is used for network monitoring. Sonicwall mails daily summary of the network usage in the form of PDF reports to the network manager(s). Most of the traffic is HTTP and FTP.

Customer has no way of figuring out which user is consuming most bandwidth since the firewall-based authentication is causing latency. Customer would also like to know how much of the traffic is business related. Additionally, they would like to address security concerns like malware, intrusion detection and be able to understand LAN traffic flows and their WAN consumption patterns in order to re-architect their network topology.

Solution

EagleEye was deployed by attaching to a SPAN port, which got all the WAN traffic mirrored. EagleEye measured levels of resource utilization such as network bandwidth consumed by the users. It extracted lots of meta data from mirrored packets. Extracted data is tightly cross indexed with flows, raw packets, security alerts etc. giving you trends driving peak utilizations; and granular insights like duration spent on social networking sites, video views etc. Over a period of few days, Customer was able to understand their bandwidth usage. A few anomalies were investigated using the forensics tools provided with the product and the firewall policies were amended. Integration with Snort and a malware plugin helped identify intrusions and enhanced security to the corporate network. Reports were generated to provide summary and detailed reports, via email, to the network managers as was being done with the existing Sonicwall tool.

Individual reports for each user also helped reducing the consumption because of increased awareness.
Eagle provided the following technological benefits:

- Analyze real time network traffic or retrospectively from hours to years. EagleEye dashboards allow user to go from high level dashboards all the way upto raw packets. This is useful for detailed forensics and to understand abnormal/suspicious behavior.
- Ultimate flexibility to measure, tag and see what the customer wanted by creating custom dashboards, alerts and reports.
- Meters 100+ traffic parameters across all network layers. HTTP traffic is further classified into various web categories which helps in analyzing employee productivity.
- Loads of tools for trend analysis, monitoring or even investigative tools helped the customer in quantifying the bandwidth usage, flow analysis led to sub-netting servers and their associated busy clients to reduce LAN congestion and finally historical data provided enough information for their capacity planning.

Benefits

- Customer was able to redesign their LAN based on the analytics provided by EagleEye. This reduced the congestion by a noticeable level.
- Additional deployments of EagleEye in the network helped them to gauge whether their ISP is providing them with the agreed upon bandwidth for both the leased lines and the backup broadband connections. EagleEye has helped them extract more from the existing bandwidth and make an educated plan for future needs.
- Threshold crossing alerts and Intrusion alerts helped the network managers in exception-based monitoring so that they can take action immediately rather than wait for users to report the problems.
- A secure SSH port to the appliance was opened to help us get into the appliance and fix issues immediately including software upgrades. This is the “Zero Touch” benefit to the customer and they do not have to worry about the ‘additional’ box in their IT rack.
- In future, if the customer decides to enforce BYOD policy then EagleEye will able to show the impact of the policy on the network by segregating the BYOD analytics from the rest of the network.

Products and services your company used

- EagleEye was deployed using a SPAN port on the Customer’s managed switch. The appliance was able to analyze a combined traffic of 20Mbps with zero impact to their network.
- Snort, the well-known open source IDS, runs on the EagleEye appliance and is integrated with the product.
- Existing Active Directory logs are pushed to the EagleEye appliance to connect users to logged in machines. Very little changes were done to the customer infrastructure while deploying the appliance.
- A secure SSH port to the appliance was opened to help us get into the appliance and fix issues immediately including software upgrades. This is the “Zero Touch” benefit to the customer and they do not have to worry about the ‘additional’ box in their IT rack.
- TeamViewer was used to train the customer remotely, on a need basis.