Netusage Alerts – NetFlow just got proactive

Netusage Alerts - Proactive Network Alerts in Real-Time.

Maintaining optimal performance from your network is a vital task within any organization. Netusage Alert helps make that task easier by proactively protecting your network from disruption. Netusage Alert is an integral part of the Netusage tools and is designed to keep your network operating at optimum effectiveness.

Proactively Protecting Your Network from Abnormal or Inappropriate Traffic.

Netusage Alerts can be triggered when traffic on your network hits different thresholds, set by the Network team. These include network traffic generated by applications, talkers, conversations and link utilization. This proves extremely useful for daily troubleshooting, capacity planning and trend analysis. It is also invaluable for identifying 'wasteful' or inappropriate traffic being run during business hours e.g. Backups. Netusage helps optimize bandwidth expenditure by sending alerts when thresholds are breached.

Extremely scalable, Netusage is used by customers globally to monitor WANs across 200+ offices, with LAN uplinks of 200+ as well. Netusage proves extremely cost effective for customers who want to be proactive to network fluctuations, not reactive.

Reduce the Risk from Network Virus Attacks

Netusage can be used to identify potential network viruses. Netusage incorporates sophisticated (real-time) detection methods to ensure that the network teams are notified as soon as a virus enters the network. This is already helping our customers to further protect their networks.

This approach helped one retail customer significantly reduce the effect and cost of a virus attack. Netusage was able to assist the engineer before the effects were felt. Here is how:

- A retail customer's network was infected by a virus
- Netusage detected an abnormal level of NetFlow Packets and ICMP Packets
- Netusage alerted the engineer to the excess ICMP application
- Netusage was used to identify the sources of this application and who they talked to
- Engineers then used Netusage to identify which circuits (hence which remote office) had been affected.
- The network was partitioned to stop the virus from spreading further
- Engineers then worked with the security team to quarantine the infected machines in a structured way.

Compare this to a scenario without Netusage, where it would be difficult for engineers to identify the source of the virus, which equipment had become infected and come up with a plan to tackle this in a timely manner. The virus will then spread further and become even more difficult to remove. Eventually the network grinds to a halt, costing the company for every hour the network is unavailable or degraded.

Integrate with Your Existing Enterprise System

Netusage employs prevailing communication methods for alerting. SNMP Trap, Syslog and email alert mechanisms are all used, as well as sending to the Netusage Alert Centre, ensuring Netusage is easily and seamlessly integrated into your company's existing monitoring systems.