Nagios Network Analyzer // Use Cases

1.888.624.4671 (US)
+1.651.204.9102 (INTL)
www.nagios.com

Purpose

This document describes several use cases for Network Analyzer and provides a general overview of the benefits received when implementing Network Analyzer.

Target Audience

This document is intended for use by IT Managers, Sales staff, and anyone looking to gain information on the practical application of Nagios Network Analyzer in their organization or IT infrastructure.

Use Cases for Managers

1. **Capacity Planning –** Use Network Analyzer to provide crucial baseline numbers and predict future bandwidth usage to aid in budgeting and financial planning. The information provided by Network Analyzer proves especially important when large hardware updates are necessary. Network Analyzer allows management to see the efficiency of the current infrastructure making it clear when additional routers, switches, and other hardware upgrades will be necessary before it becomes a problem that affects the business.

2. **Secure Intellectual Property and Identify Corporate Data Leaks –** Network Analyzer is essential in detecting and preventing intellectual property theft and corporate data leaks. Network Analyzer allows you to view the conversations taking place on the network. If an unidentified device is connecting to the company's network, or suspiciously large amounts of data are being transferred from the network, Network Analyzer can immediately alert a relevant IT staff member to promptly address the problem.

3. **Setting QoS Baselines –** Prioritizing application bandwidth usage is crucial in any environment, but especially in large corporate infrastructures, setting Quality of Service baselines is critical. Network Analyzer is designed to make it easy to view large amounts of data and quickly diagnose the health of the network. By implementing Network Analyzer, you can quickly identify bandwidth allocation across the network to determine who and what is taking up the most bandwidth. This makes it easy to establish Quality of Service permissions on your network.

Use Cases for Managers

1. **Detecting Security Breaches and Unauthorized Access –** Network Analyzer gives system administrators and IT Staff the tools necessary to determine exactly where potential security threats can arise. Monitor specific ports and track communication between devices to see who is accessing the network and whether those devices are authorized to do so.

2. **Detecting Viruses and Malware –** By monitoring commonly accessed malware and virus ports, Network Analyzer makes it easy to determine if a network has been compromised. When combined with Network Analyzer's built-in bandwidth spike alerts, you'll always be notified when potential threats arise, which saves your team time and allows them to resolve the issue.

3. **Determine Bandwidth Usage by Device, Customer, or Switch Port –** For Internet Service Providers who bill on a per MB data plan basis, it is crucial to have an accurate representation of the network traffic being used. Network Analyzer provides in-depth granular reports that can determine exactly how much data was being used by that device or customer. Network Analyzer can provide ISPs with the information necessary to bill their customers with pinpoint accuracy.