



# Achieving Predictive Management with Robust, Flexible Early Warning Alarming

Despite all the enhancements and improvements in network redundancy and self-healing IT initiatives, end users regularly feel the effects of service delivery slowdowns. While the experience of actual hardware outages has been effectively addressed and are rarely noticeable to the end user, service delivery can still feel slow as a customer checks his order status or a purchasing agent places a just-in-time delivery request for manufacturing inventory. These same end users are still, despite all these technological advancements, the first to know there is a problem.

This paper will describe how to use the nGenius® Service Assurance solution to gain visibility into the services being delivered across the network and how to harness that information in such a way as to gain earlier notification of degradations in order to prevent broader service meltdowns.

## Business Challenges

Today's high speed, global networks are host to complex, revenue-carrying services, financial trading orders, virtualized order processing applications, cloud-based CRM (customer resource management) services, patient-care electronic records and medical images, as well as converged, latency-intolerant voice and video. The advent of cloud computing and Software as a Service (SaaS) applications to support cost-effective delivery of business services underscores how important these services have become – they represent millions of dollars in client portfolios, high-value product revenue, safe and rapid patient treatment, and quality phone conversations with customers and partners. Disruptions as minor as millisecond delays, or as dramatic as hours of complete application unavailability can mean severe financial loss, irreparable customer dissatisfaction, or even health care implications.

It is therefore no surprise that business processes and IT service delivery are rapidly becoming inseparable. To be competitive, organizations need to maintain high service delivery and application availability. Further, these organizations require visibility into the services as they are being delivered to the end users in order to forecast when subtle changes in traffic behavior may be predicting a more ominous threat to the efficient performance of essential business services.

One of the fundamental problems is that IT organizations often find themselves reacting to end user reports of application slowdowns. In the strict "up, down, broken" analysis of the elements of the network, everything looks fine. One group in IT will check the routers, switches, load-balancers and report nothing is down, all systems running fine. Another group will state the application servers and databases are all operating efficiently. Another will rule out the client workstations as the source of the slowdown, no spyware or viruses. In other words, all systems are green. And yet, the end user's experience is still poor, in fact, many users may be affected by the situation.

Understanding possible influences to optimal service delivery means focusing on the internal and external factors that impact service quality, availability and end user experience. Application and network performance is an important aspect, however, such things as threats, undetected attacks and traffic violations also has a significant impact a user's experience with service delivery.

The question then becomes, how to diagnosis a slowdown or poor user experience when the elements of the system appear fine? The answer is in the communications amongst and between these individual elements. The network vantage point provides services-aware visibility into the delivery of applications to users throughout the network. End user demand, bandwidth capacity, traffic patterns and behavior are revealed from this vantage point. Tracking and analyzing this data and applying a variety of methods for identifying and alerting on degradations and disruptions will help IT organizations predict which minor issues may be forecasting more catastrophic events early enough to prevent the kind of meltdowns we all read about on the Internet.

## Packets Represent the Best Vantage Point

To meet the business challenges described head on, IT organizations need two things – first, visibility into actionable data with which to apply the second element – establishment of a set of alarms with which to detect, predict and prevent service-impacting application disruptions. Packet-based data flowing between switches, routers, servers, databases, and end user workstations should be leveraged as the best source of operational intelligence in order to gain the visibility necessary to see these essential applications and services.

NetScout® has developed technology to passively monitor the packets traversing the global, modern IP networks. The nGenius Probe, nGenius Integrated Agent, nGenius Virtual Agent and nGenius InfiniStream® data sources are non-intrusive, high performance, real-time and historical monitoring devices. They leverage packets as the best data source to collect and analyze such metrics such as traffic and application utilization, network talkers, conversations, error conditions, response time, and on-demand packet captures. Packets not only offer a better,

more complete method of application identification of such key applications as web-based cloud services and voice (VoIP) convergence services, they also reveal potential threats or undetected attacks and traffic violations. The nGenius InfiniStream data source offers the additional capability of continuously capturing and storing the packets with essential header and payload information that can be used for post-event forensics.

With packet-based data collected by nGenius Probes, nGenius Integrated Agent, nGenius Virtual Agent and nGenius InfiniStream devices, IT organizations can use nGenius Service Delivery Manager and nGenius Performance Manager software with sophisticated analysis to perform real-time analysis and alarming on predictors of degradations as well as early warning indicators of potential threats, undetected attacks or traffic violations.

**Evolving a Proactive, Predictive Process of Service Delivery Management**

Enterprises are engaged in expensive, mission-critical IT projects and are rolling out the very latest in data center virtualization and cloud computing environments. Due to the amount of redundancy and re-routing architected into these networks, actual hardware or circuit outages are often undetected by the end users. Thus, the bigger challenge is how to address the often persistent and unrelenting intermittent services degradations and threats to overall high quality experience that represent an even greater threat to the business and end users – particularly revenues and customers.

A no less important challenge is who in the IT organization may be most helped by the information related to the degradation. Depending on the quality of the fault information, root cause may be pinpointed, or at a minimum, immediately rule out parts of the network. Operating the fault detection analysis across one common data collection platform, the nGenius Probes, nGenius Integrated Agent, nGenius Virtual Agent and nGenius InfiniStream devices, provides a single source with which network faults, such as dropped packets, as well as application-related faults, such as server errors like Error 500s can be triggered. When the overall IT organization are all resourcing the same common set of nGenius solution information, they can much more easily and effectively collaborate on resolving the causes of the faults.

The increased dependency on business services today has created an imperative to avoid disruptions. Thus, the challenges to IT organizations:

- Detecting and preventing application service disruptions and degradations in their earliest stages in order to aid in diagnosis – this will shorten the time to pinpoint the source of the problem so corrective actions can be undertaken before the business experiences a broad outage. Revenues, customer satisfaction and employee productivity tied to use of critical services will all be direct beneficiaries to solving this challenge.
- Moving from a reactive to proactive service delivery management of their global networks. The benefits of proactive management are IT productivity as well as IT staff workload and job satisfaction.

What is needed is the nGenius Service Assurance solution, a centralized viewpoint into all conditions impacting service delivery. A broad range of mechanisms for alerting on a variety of violations is required that includes support for traffic utilization thresholds, time-over-threshold violations, anomaly behavior alerts, discovery alerts, error code alarms and key performance indicator (KPI) alerts, which when combined, deliver the most robust, complete coverage for the variety of threats to optimal service delivery facing most global organizations.

**nGenius Service Assurance Solution Overview**

NetScout has focused the nGenius Service Assurance Solution on using the data collected by nGenius Probes, nGenius Integrated Agent, nGenius Virtual Agent and nGenius InfiniStream data sources to identify problems earlier, aid in diagnosis, and shorten the time to pinpoint the source of the problem so corrective actions can be undertaken before the business is impacted. The nGenius Performance Manager provides basic, actionable intelligence through threshold-based alarming as well as a unique time-over-threshold alerting with which IT organizations learn of segment congestion or application slow-downs.

nGenius Service Delivery Manager is a software application that applies an advanced level of analysis against the same packet data collected by the nGenius data sources. nGenius Service Delivery Manager offers two types of alarming, the first, an advanced, automated early-warning analytic engine to identify traffic anomalies that may be indicators of emerging issues. Key performance indicators, or KPIs, are the second advanced alarming capability delivered through nGenius Service Delivery Manager. On an application-basis, KPIs are configured to analyze the data to reveal client and server errors, application slow-downs and outages, and packet loss for the application.

The unique combination of analysis found in nGenius Performance Manager and nGenius Service Delivery Manager provides the most complete approach to alerting IT organizations of issues so they can advance their efforts for protecting and preventing catastrophic meltdowns.

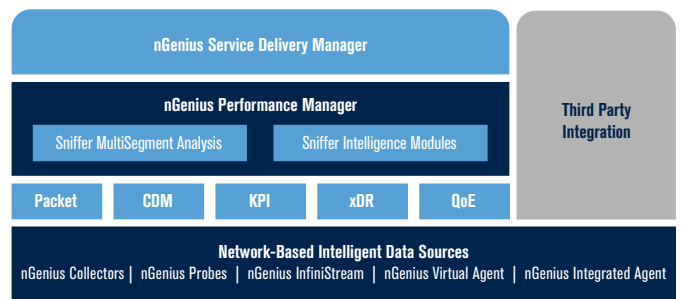


Figure 1: nGenius Service Assurance Solution architecture

## Proactive Alerts in nGenius Performance Manager

The ability to identify a network fault and react to it has been a long-standing function of nGenius Performance Manager. Unified service delivery management focuses on a more proactive method to preventing disruptions and managing faults by continuously monitoring for conditions that indicate an emerging problem, threat or degradation. This proactive approach is essential to reducing poor end user experience and service interruption.

The nGenius Performance Manager is employed to evaluate overall segment utilization, application utilization and trigger a threshold-based alarm as well as analyze utilizations and response time levels over a configured period of time to activate the unique time-over-threshold alerts. As a minimum, this represents the necessary levels of analysis and alerting to help IT organizations rapidly attack segment or virtual circuit congestion or application slow-downs.

### Rising and falling threshold alarms

Traffic statistics can be used by the nGenius Performance Manager to create alarms when utilization, errors or congestion levels exceed acceptable thresholds over the data link, network and application layers. Threshold alarms are best set at the user impact level therefore allowing you to see priority. At the point threshold alarms are reached, they require immediate attention because the users are feeling the effects.

Setting thresholds of network activity to identify resources at risk of failure the instant the threshold is reached is key to acting on the problems and ensuring that corrective actions be immediately applied to minimize poor delivery of networked business services. Static threshold alarms on rising network utilization or degrading application response times enable rapid corrective actions.

nGenius Performance Manager, in combination with strategically deployed nGenius data sources, support threshold setting and immediate alarming on network and application statistics, including the following alarming capabilities:

- **Traffic utilization threshold alarms:** Identify potential areas of congestion, such as 85 percent utilization on a particular segment, or indicate potential failures, such as the disappearance of traffic on a load-balanced link
- **Application service threshold alarms:** Triggers a threshold alarm when a particular service volume, like RTP, exceeds 10 percent utilization of the segment; thresholds on application utilization can also identify undesired traffic patterns, e.g., increasing amount of peer-to-peer traffic, or an undesired network usage, e.g., YouTube traffic
  - Application-based alarming can also be set against IP\_OTHER; this delivers immediate identification of new applications as they first appear on the network. Alternatively, this may discover and alert the IT staff to a new virus activity or the actions of malware
- **Virtual circuit-based application service threshold alarms:** Configurable by virtual interfaces, such as VLANs, MPLS Sites, or QoS classes, this alarm can be triggered when a particular service volume, such as a financial market trading feed that drops below 250 bytes for an MPLS site

- **Application response time alarms:** Establishes alarm thresholds for response times of particular applications, such as if the e-mail application expands beyond 800 milliseconds or if the CRM application takes more than 450 milliseconds

Because a single characteristic of “normal” network traffic can't be determined, thresholds alarms are often difficult to set. For example, if thresholds are set too high problems may be missed or seen too late. Set them too low and the volume of alerts can be overwhelming. Turn them off altogether and risk missing critical notifications that could avoid serious service degradations or outages.

Using the nGenius Performance Manager, with historical reporting and trend analysis, highly granular, automated, daily, weekly, and monthly reports are generated which can be configured to track segment utilization. These can be invaluable in determining where to set utilization threshold alarms. For instance, if it is revealed that typical utilization on the links to the data center are 55 percent, with spikes to 85 percent, an IT organization may determine the 5 points below a spike will be their policy for setting threshold alerts.

### Benefits of Threshold Alerts

- Minimize risk of catastrophic failures by quickly responding to congestion issues with immediate notification of high overall segment traffic utilization
- Improve IT productivity by reducing time to pinpoint problems using virtual circuit application alarms that reveal source of increased application traffic volumes
- Reduce end user impact by improving time to resolve service degradations with analysis and notification of that application response times are experiencing slowdowns

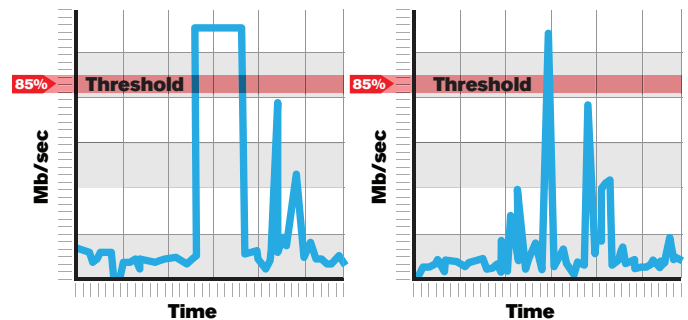


Figure 2: Threshold Alerts Figure 3: Power alarms –Time-Over-Threshold Alerts

### Threshold Alerts in Practice

One financial services company had a process problem in their IT organization. The application developers were releasing new applications onto the production network without properly notifying the network team. As users would conduct business with the new application services, they would report troubles that the network team were challenged to resolve.

By establishing an application threshold alarm in nGenius Performance Manager on IP\_Other traffic at 1 percent, as soon as a new application was introduced, the network team was alerted. Armed with this information, the network team could configure targeted monitoring of the application service and associated response time power alarms.

### User-defined, Time-over-threshold Alarms

Typically, when threshold alarms are generated, the associated trap message contains only the information that a threshold has been surpassed or a response time has been crossed, with no further instruction on the potential problem cause. While important to know of the threat, there are a number of hidden contributors to any rise in traffic utilization or business service degradation. Intelligent alarming establishes a context for the fault, revealing what circumstances led to it, what was going on at the time, and what applications and users were affected. In fact, if evidence of what is occurring during a performance event were attached to the alarm, along with the ability to directly link into contextual data to facilitate the workflow, excessive process cycles can be removed from the troubleshooting process.

Power alarms are an intelligent alarming concept that pinpoints the source of the problem. The innovative power alarms of the nGenius solution are based on a time-over-threshold settings that filter out spurious notifications typically caused by routine traffic spikes and focuses on sustained situations. Once a threshold has been exceeded, a single alarm is sent to the nGenius Performance Manager that includes the event violation along with the state of every application, host, and conversation that may have caused it. This valuable data is saved for immediate retrieval by nGenius Performance Manager. While power alarms are based on proprietary NetScout technology, as part of the CDM technology, it uses standard SNMP mechanisms to send the trap and to retrieve the associated evidence.

Power alarms are supported for utilization, response time and availability threshold-based notifications. These are the conditional and evidence-gathering alarms available in the nGenius Solution:

- **Traffic utilization power alarms:** Power alarms are time-over-threshold alarms which collect evidence regarding what has contributed to a performance event. When a threshold is crossed and sustained over a user-defined period of time, nGenius Performance Manager receives an alarm with evidence associated with the event. Evidence includes top applications, hosts and conversations that contributed to a utilization threshold. For instance, a power alarm could be established on a segment that sustains 80% utilization for a full second.
- **Response time and availability power alarms:** Application response time alarms, set on an individual application basis, alert when an application is approaching poor performance, such as a one second response time for an application that typically responds within 800 milliseconds. If this alarm is generated, the trap will include the slow down information, along with the hosts and conversations associated with alert.
- **Microburst power alarms:** Traffic microbursts can severely disrupt the flow of time-sensitive applications such as voice over IP, streaming financial market data, or trading applications, yet are often hard to detect or diagnose. The nGenius Performance Manager solution can detect and alarm on a millisecond-long burst of activity and gather evidence during the user-definable alarm interval.
  - The nGenius Solution generates microburst power alarms based on very quick bursts in traffic rates. The interval can be configured from between 10 milliseconds and 100 microseconds on either physical or virtual interfaces. Evidence is launched based on the services and flows running during the alarm time.

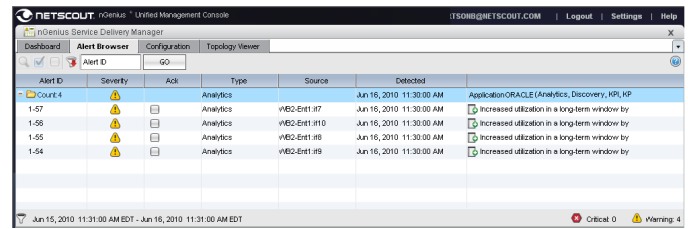


Figure 4: nGenius Service Delivery Manager coalesces all threshold, power, anomaly and KPI alerts for viewing in the alarm viewer.

Alarms do not typically occur as an IT professional is monitoring the very link, circuit, host, or business service creating the point of fault. Therefore, the unique power alarms provide those eyes and ears on the network to offer evidence essential to diagnosing the causes.

### Benefits of Power alarms

- Better and faster diagnosis of the cause of traffic congestion by retaining the data regarding the top users and applications contributing to the utilization at the time the event occurred.
- Improve IT productivity with more focused troubleshooting by delivering evidence surrounding application degradations
- Reduce unproductive efforts associated with multiple, isolated traps by offering a single “over time” alarm.
- Optimize delivery of time-sensitive applications, e.g. voice or streaming financial market data, by discovering evidence of hard-to-pinpoint microburst events.

### Predictive Alerts Available nGenius Service Delivery Manager

nGenius Service Delivery Manager extends the basic proactive threshold and time over threshold alarming of nGenius Performance Manager to more sophisticated, predictive and preventative analysis. nGenius Service Delivery Manager is software that resides on the nGenius Performance Manager server and applies patented, statistical behavior modeling and anomaly detection to the same packet data collected by nGenius Probe, nGenius Integrated Agent, nGenius Virtual Agent and nGenius InfiniStream data sources strategically deployed throughout the network.

nGenius Service Delivery Manager offers an advanced, automated early-warning analytic engine to identify traffic anomalies that may be indicators of emerging issue as well as application-based KPI metrics and alerts that combined give IT organizations a real chance of catching issues at their earliest stage of development when there is a chance of preventing end user impacting degradations.

### Automated, Behavioral-Based Anomaly Analysis

Baselining is the process of measuring “normal” network and application behavior so that future anomalous behavior can be determined. But how do you account for all the variables that define normal behavior? Network traffic is continuously changing – from day to day, week to week, even season to season – making it tricky to establish what is anomalous and what is normal for any given day and time. For example, is the Tuesday morning spike due to a customer database query gone awry or an increase in customers checking their order status? Is Friday afternoon’s blip due to a

well-attended marketing webinar or is it the result of a regularly scheduled backup that should really be moved to non-peak hours?

nGenius Service Delivery Manager automatically learns a network's normal historical patterns of behavior, then compares the current activity to the baseline to identify changes in network activity without the manual configuration and guesswork of setting thresholds. When an anomaly is discovered, a trap alert is triggered in nGenius Service Delivery Manager. nGenius Service Delivery Manager can group related alerts and provide detailed information regarding the offending physical links, virtual circuits, QoS classes, applications and key performance indicators (KPIs). Armed with this information, the IT organization can often act to resolve performance issues before business services are impacted.

Once nGenius Service Delivery Manager detects a behavioral anomaly, it correlates the anomalous behavior to the offending links, applications and KPIs:

- Monitors high-level KPIs that are derived from packet analysis and which focus on overall network performance from the perspective of end user experience. The KPIs are based on packet data, and is not simulated data, sampled, nor artificially skewed by data reduction. As such, these top-level service health views are extremely precise and contextually linked to the true source of operational intelligence – the network packets themselves.
- nGenius Service Delivery Manager takes the guesswork out of the troubleshooting process by linking the health of the environment to the packet-level details and providing a streamlined workflow to quickly access the details when necessary.

IT organizations can increase application availability with earlier warning and by linking the alarms with detailed diagnostics information, network and operations managers can act to resolve issues before users are impacted. When an IT organization has a policy of centrally managing network events, the intelligent alarms can be sent directly to the fault management platform of choice.

A congestion meltdown at the campus headquarters was avoided with anomaly analytics and end- users were able to continue serving customers, taking orders, and shipping products.

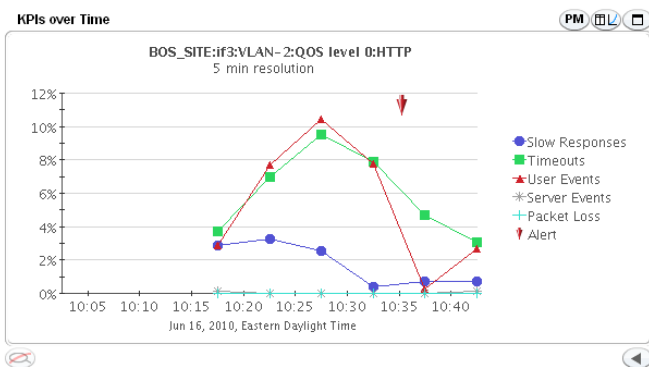


Figure 5: Anomaly Alert – nGenius Service Delivery Manager discovered and alerted on a deviation in normal behavior for HTTP traffic, for higher than normal time outs and user events.

### Benefits of Anomaly Alarms

- Enable preemptive intervention with early-warning notifications to predict and prevent service degradations and outages
- Avoid user-impacting meltdowns with automated analysis of network behavior and relationships to streamline root cause identification and minimize time spent on problem identification
- Improved user experience and employee productivity by providing IT managers links between the anomaly alarms and detailed diagnostics information so they can act to resolve issues
- Superior service delivery management by detecting the elusive issues, often left undetected by other solutions, e.g. “drifts in traffic” or application utilization over time that can significantly disrupt services performance
- Improve IT productivity by reducing unproductive and disruptive activity associated with multiple isolated traps by offering a single over time alarm.

### Anomaly Alerts for Threat Management

IT teams face daunting security challenges today, whether they are external or internal forces at work and be them unintentional or malicious in nature. It is becoming imperative that organizations have the highest quality data to help identify these potential threats. Because networks are faster than ever before, when a threat or security problem does occur it can be populated throughout the organization rapidly.

The nGenius Service Assurance solution is effective in augmenting an existing security initiative either by identifying abnormal situations as they arise, or in researching suspicious traffic patterns as potentially nefarious. Identifying and analyzing these packet-flow streams enables quick classification of the activity or transaction to rapidly take action when an attack in its tracks. The nGenius Service Assurance Solution can provide early warning of security-related performance problems using historical and real-time data to accelerate assessment and remediation of security issues with a network-wide viewpoint and easily configurable packet capture and decode capabilities for post-event forensics and root cause identification.

### Anomaly Alerts in Practice

The security team of an enterprise was loading new virus software on all the workstations at one of their campus locations. Once installed, the client would notify the server it was ready to receive the configurations. The configuration downloads were bandwidth intensive and had the potential to quickly impact end users as they tried to look up customer records, product inventory and shipping dates. However, the nGenius Solution with anomaly alerts notified the IT organization of the abnormal behavior as it analyzed the difference in both the type of traffic and volume at that time of the day. The security team was notified and the automated configuration feature was disabled until a low peak time of the day when users would not be impacted.

The nGenius Service Delivery Manager, nGenius Performance Manager and nGenius Intelligent Data Sources combine to deliver the nGenius Service Assurance solution which effectively supplements an existing security solution with discovery and traffic violation alerts. Discovery alerts of new applications, servers and users and traffic violation alerts that recognize unauthorized use of the organizations services enables the nGenius solution to bridge network and security operations teams and empowers them to:

- **Recognize deviations from normal traffic behavior of application servers and application hosts**, such as traffic and connection volume changes, excessive errors, TCP resets or TCP retransmissions that are all early warning indicators.
  - Identify Risk of: Denial-of-Service floods, Point to point (P2P), or Behavior associated with BotNets
- **Discover new application servers**, such as the appearance of a new host or server, any changes in host or application behavior based on the IP addresses in use, provide early warning indicators of potential threats.
  - **Identify Risk of:** Server or host hijack, Data theft, or Infiltration of a server
- **Identify traffic violations to user defined policies**, that may include discovery of restricted applications on a subnet, unauthorized access by a user to a sub-net or a server, or unsupported applications on a desktop all of which are early warning indicators.
  - **Identify Risk of:** Unauthorized logins on SSH/FTP, Unauthorized social networking, Unapproved Streaming video

Essential to making this solution effective for threat management is the nGenius InfiniStream appliance, with recording and archiving of continuous packet capture trace files, including full packet header and payload details on a 24x7 basis, enabling long-term recall for post-event forensics analysis and event reconstruction. The nGenius Service Assurance Solution leverages automated behavior analysis and monitoring capabilities against a customizable set of defined rules to provide threat management functionality with a correlation of anomalous events discovered by an existing security tool and observed network traffic behavior. Since the nGenius Service Assurance Solution is complementary to signature-based security solution, this additional level of analysis proves its value when a previously undetected or unknown threat enters the environment and bypasses the signature-base solution that did not know to look for it.

**Benefits of Anomaly Alarms for Threat Management**

- Offers an extra layer of security over existing solutions with discovery alerts to new applications and new servers that results in reduce risk and impact
- Complements existing security solutions by identifying anomalous behaviors of undetected or unknown threats, where pattern matching has not been possible yet thus pinpointing emerging and blended threats
- Improves IT staff productivity by automating analysis of all monitored traffic to provide early warning of potential threats, internal or external, resulting in shorter time to respond to threats that have a far greater scope of damage to the organization

**KPI Alarms**

Traditional traps and alarms are simple in their analysis of the network – has a threshold been reached that the IT staff or company deems enough of a concern to warn against? However, more questions typically plague an IT organization as it attempts to deliver business services to their end users. How fast is each application running? Is that response time acceptable? Are there any errors for that application or network area? What is the application delivery success rate? Is voice quality acceptable? If these questions could be answered by setting configurable alarms that advise the IT staff when service delivery performance is in risk of degradations, then perhaps they could be prevented.

NetScout has developed key performance indicators or KPIs to help meet the challenge of predicting and detecting application performance issues and ultimately preventing outages.

KPIs measure errors, packet loss and response time degradations for key applications and together provide an indication of end user experience. KPIs provide essential information for:

- Monitoring response time and evaluating if the response time falls within acceptable parameters
- Determining if client or server errors exist. By looking at the success rate for applications or servers processes, nGenius Service Delivery Manager provides IT with an indication of where potential problems may exist
- Providing an assessment of the quality of voice or multicast applications by analyzing packet loss measurements

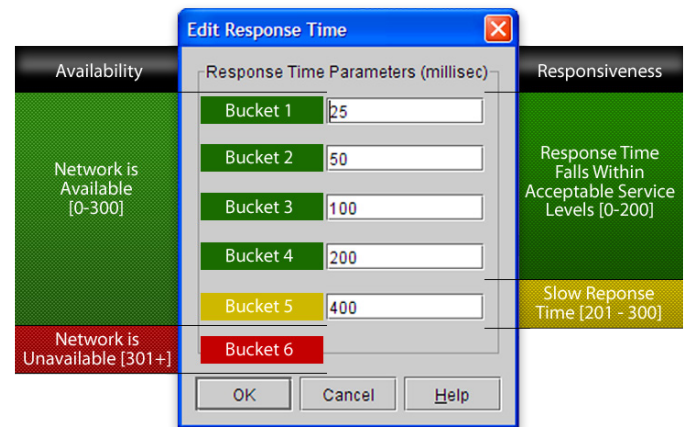


Figure 6: User configurable Response Time KPI alert

**Types of KPIs Available**

The nGenius Service Assurance Solution has adopted easy-to-interpret views of KPI metrics that provide vision into the health of applications and end user experience. KPIs are defined on a per-application basis on five-minute samples and can only be tracked on applications that are enabled for response time monitoring. KPI alarms are based on how often a threshold is violated, how many user or server errors occur or when a certain number of packets are dropped during a five-minute interval. For example, if the user events KPI alarm value is set to “5” for HTTP, then when five 400-type errors occur in a five-minute sample, a KPI alarm is generated.

For data applications, the following alerts can be configured:

- **Slow responses** — Application response that exceeds a preset threshold for acceptable responsiveness when users will feel a slowdown while using the application; e.g. five times over 500 milliseconds
- **Timeouts** — Application response that falls outside a predefined timeout limit that effectively feels to the end user as though the application is essentially unavailable; e.g. response times are beyond 750 milliseconds 10 times
- **User Events** — Application-specific client errors (varies by application, e.g. HTTP 4xx)
- **Server Events** — Application-specific server errors (varies per application, e.g. HTTP 5xx)
- **Packet Loss** — Dropped packets in VoIP protocols and IP Multicast applications

The nGenius solution has incorporated a number of specific KPIs that can be configured to track user events, server events for SIP, HTTP, DNS, and AAA services – Radius & Diameter, as well as Packet loss for VoIP protocols and IP Multicast applications.

For enterprises with converged networks, the nGenius solution offers a variety of focused KPIs to track for evaluating IP voice issues. The KPIs that track timeouts and slow responses for application response time measurements equate to max jitter and high jitter metrics when monitoring for voice. The expectation with the addition of voice to business data traffic is that the voice quality will be as good as its analog predecessor. Packet loss, a known factor in every network, can impact that quality. Therefore, targeted, focused analysis against these metrics is essential to stay ahead of poor quality voice in converged networks.

**Error Code Alarms**

Error code alarms are vital to any organization that relies on Web-based or client/server services such as healthcare organizations that leverage their Web sites for out-patient care assistance, e-commerce retailers, insurance companies offering auto and homeowner insurance quotes online, retail banking organizations and any SaaS organization. When armed with a better understanding of the “types” of server and user errors that are occurring, problem resolution is more efficient. Identification and speed are critical elements here as often the individuals impacted are customers or potential customers who rather than reporting a problem are more likely to move to another company’s Web site.

Error code alarms are designed to provide a granular view of server and user events, offering a deeper insight into what is impacting service delivery. The nGenius Service Assurance Solution:

- Identifies the particular errors, such as 40x or 50x errors in HTTP traffic
- Error code distribution, such as how many 401 vs 404 errors seen
- Classify the servers, users (clients), and conversations that have seen particular error codes, e.g. which servers are seeing the 404 “Page not Found” errors

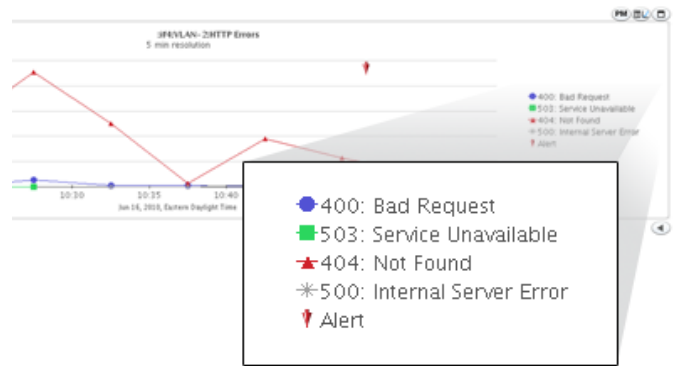


Figure 7: KPI Alert – nGenius Service Delivery Manager analysis of HTTP traffic reveals client 40x and server 50x errors that may impact user experience with web-based services.

**KPI Alerts in Practice**

A global leader in home products manufacturing encountered a problem with a newly implemented, Web-based, product management application developed by a third party partner. Remote users were experiencing slow response times when accessing the application, however, the local users felt the quality was fine. The application development partner attributed the response problems to the third-party WAN service provider, perhaps bandwidth congestion was the cause. But a review of WAN link and application utilization showed that all were operating within normal parameters.

nGenius Service Delivery Manager, through a KPI alert discovered an abnormally high number of user event errors compared to the number of transactions. The client errors were causing an increase in slow responses and time outs, which were more noticeable to the remote users over the WAN than the local users on the high-speed LAN. Armed with the details of the problems, the network team was able to collaborate with the application development partners to rectify the problem, thus improving the end user experience of the product management application for the employees using it at the remote locations.

**Benefits of KPI Alarms**

- Optimize business service delivery and application availability with warning of specific slowdowns or unavailability of key business applications before they degrade
- Improved user experience by analyzing user or client events as well as server events, providing IT managers essential diagnostics information for pinpointing the cause of the problem
- Improve IT productivity by using configurable, targeted alerts for the applications and business services most important to each organization’s network
- Maintain high quality voice delivery in converged networks with focused analysis on packet loss, high jitter and max jitter metrics

### Integration with Third-Party EMS

Network operations groups working with well-known element management systems (EMS) are often hard-pressed when it comes to resolving application and services degradations. They are the very operators researching across the infrastructure end user reported issues, finding the networks, servers and end user workstations all operating "in the green." The vantage point from which the nGenius solution watches the traffic flows between those elements in the network provides these network operators, and their other IT colleagues, precisely the information they need to pinpoint the elusive application slowdowns.

Historically, sharing trap information with third-party EMS systems was the integration practice of many network performance systems. However, it was limited, one-way information lacking even basic context about the incident with which to start troubleshooting. NetScout developed a new approach with the highly-qualified alarms described herein and implemented bi-directional exchange of alarms and detailed information between the nGenius solution and third-party EMS such as HP Network Node Manager and IBM NetCool. Alarm messages are embedded with plain-text descriptions and URLs that launch context-sensitive graphs into nGenius Service Delivery Manager or nGenius Performance Manager for easy drill downs into additional details. The centralized views of alerts in the EMS system with contextual drill downs to root cause of the alerts in the nGenius solution are making network operators and their IT counterparts more efficient in their overall problem resolution workflow processes.

### Summary

IT organizations today are delivering essential business services over the fastest, most complex networks to date. They simply cannot wait around for end users to call complaining of poor response times or slowness with their experience on the network. And let's face it – customers don't bother calling, they simply change vendors.

The ability to identify a network degradation or fault and react to it has been a long-standing function of service delivery management. More proactive approaches, however, need to be employed to enable IT organizations to evolve to the level of preempting or preventing disruptions. This will require continuous monitoring for conditions that indicate an emerging problem or degradation.

The nGenius Service Assurance solution provides accelerated fault detection as part of its unified service delivery management solution. With strategically deployed nGenius data sources throughout the network in combination with the nGenius Performance Manager and nGenius Service Delivery Manager, IT organizations can provide improved services delivery, enhanced employee productivity, and more efficient IT productivity by leveraging threshold-based alarms, response time alarms, time-over-threshold-based alarms, anomaly alarms and KPI alarms. This predictive and preventative approach is essential to reducing service interruption and rectifying potential issues which ultimately improves end user experience, business productivity and profitability.

Type	Features	Value	Alarm Delivery
Threshold	Basic alarm  Example: Response time exceeds 400ms	Set at high-water mark to catch outages	Immediate
Power	Highly granular (microburst); Captures trigger info	Real-time; identify service outages; support SLAs	Immediate
KPIs	Triggered on how often a threshold is violated  Example: The number of times that response time exceeds 200ms is greater than 5	Indication of users experience; provides additional level of control vs. threshold alarms	Threshold KPI alerts are immediate
Analytic Alerts	Dynamic, intelligent, self-adjusting; can be based on user definable parameters / KPIs; Provides evidence  Example: Today a new application server was discovered in the network.	Early warning system	Analytics alarms 15 minute delayed



#### Corporate Headquarters

310 Littleton Road  
Westford, MA 01886-4105  
Phone: 978-614-4000  
Toll Free: 888-999-5946  
www.netscout.com

#### European Headquarters

One Canada Square 29th floor  
Canary Wharf  
London E14 5DY  
United Kingdom  
Phone: +44 207 712 1672

#### Asia/Pacific Headquarters

Room 105, 17F/B, No. 167  
TunHwa N. Road  
Taipei, Taiwan  
Phone: +886 2 2717 1999



**For more information  
please visit [www.netscout.com](http://www.netscout.com)  
or contact NetScout sales at  
800-309-4804 or +1 978-614-4000**

© 2010 NetScout Systems, Inc. All rights reserved. NetScout, nGenius, InfiniStream and Sniffer are registered trademarks, and the NetScout logo is a trademark of NetScout Systems, Inc. and/or its affiliates in the United States and/or other countries. All other brands and product names, and registered and unregistered trademarks are the sole property of their respective owners. NetScout Systems, Inc. reserves the right, at its sole discretion, to make changes at any time in its technical information, specifications, and service and support programs.