



Filtering and Expert Analysis Speed Resolution of Intermittent Performance Problems



Filtering and Expert Analysis Speed Resolution of Intermittent Performance Problems

Executive Summary

This white paper will explore how the nGenius® InfiniStream™ appliance's intelligent Deep Packet Capture, data mining and filtering capabilities can be used to speed the investigation of network and application performance issues. The second half of this paper uses a real-world case study to illustrate how the nGenius InfiniStream appliance was used to troubleshoot an intermittent performance problem that was causing significant dissatisfaction and frustration with the users of a financial analysis application.

Speeding Investigation of Network and Application Performance Issues

Diagnosing and troubleshooting subtle or intermittent application and network problems or security issues that occurred overnight, the previous day, or even over the weekend can be virtually impossible or, at the very least, extremely frustrating without the proper tools. For the most critical areas of the network – those with revenue-impacting services – IT cannot afford to spend time manually recreating a problem, wading through log files, or waiting for a problem to recur (if it ever does). Intelligent Deep Packet Capture technology is designed to facilitate retrospective or “back-in-time” problem resolution by capturing packets and storing them for later availability and analysis.

NetScout nGenius InfiniStream technology pairs a traditional packet capture device with terabytes of disk space, intelligent filtering and robust data mining to facilitate problem isolation and resolution. This solution can help network managers determine the root cause of a performance problem – accelerating the time to resolution and enabling changes that make future occurrences much less likely.

Finding Elusive Problems

Intermittent network events can be extremely frustrating and time consuming to diagnose. Because they are fleeting, they are almost untraceable and extremely difficult to diagnose with traditional portable network analyzers. Often times when IT receives complaints that the network is slow, the engineer that goes out to analyze it on location finds nothing. Persistent faults with stable causes are more easily found and more readily resolved; faults that pop up and then disappear leave engineers unable to follow the generic process of elimination that is inherent in all troubleshooting, and thus are far more difficult to identify and address.

Typical intermittent network problems might include application design issues, load balancing problems, router mis-configurations or errors, DNS issues or mismatched QoS levels.

Certain security events can also cause considerable consternation for network and security managers. Despite the best efforts of network perimeter defenses such as firewalls and network intrusion detection or prevention systems, networks occasionally still come under attack. The culprits that typically slip through defenses, because of their elusive nature, include:

- Rogue wireless devices
- Trojans or worms introduced via laptops, personal email services or flash-based storage devices
- Zero-day attacks for which signatures have not been implemented
- Unauthorized remote control “zombie”, denial of service (DoS) attacks, or peer-to-peer software



The Power of Dynamic Data Mining

Troubleshooting complex network environments often hinges upon whether or not a network engineer can focus in on the appropriate packets that will enable him to identify the root cause of the problem. The first step in the process is to capture 100% of the packets traversing the network segment in question to enable forensic analysis. The second, and more challenging step, is mining and analyzing the packets to reveal critical insight to network and application elements and behaviors.

A variety of data mining capabilities can be used to quickly derive actionable information from captured traffic, such as:

- Expert views with drill-downs to graphically analyze captured packets and hone in on the exact time, user or application associated with the network disturbance.
- Pre- or post-capture filters to create custom rules to identify the precise combination of addresses, ports, applications and patterns for network and security-related events.
- Detailed packet decode functionality to perform in-depth analysis and playback of selected packets.

Filtering plays an especially critical role. In most cases, the majority of traffic on a network experiences no problem, but the traffic that does experience delay or performance issues is where an engineer spends 80-90% of his time troubleshooting. Improving an engineer's ability to filter traffic appropriately in a troubleshooting scenario has the tangible effect of reducing the time spent responding to problems and consequently increasing the time available to proactively prevent new issues from happening. From a business perspective, the benefit is accelerating the resolution of critical issues, thereby shortening the impact on productivity or revenue.

nGenius InfiniStream Appliance Facilitates Forensic Analysis

For network, application and security issues, network operators and security administrators can use the continuous traffic recording and analysis capabilities of the nGenius InfiniStream appliance to pinpoint root cause, perform detailed analyses, and identify affected hosts to solve problems that happened in the past or are currently occurring.

The nGenius InfiniStream family provides always-on intelligent Deep Packet Capture (iDPC) capabilities with a scalable recording capacity ranging from 500GB up to 15TB of storage for collecting and storing packets that traverse the network. Continuously capturing and storing all packets ensure that critical packet-level details are available for replay whenever a problem occurs.

Sniffer Intelligence

NetScout's industry-leading Sniffer Intelligence solutions – Sniffer Intelligence, Sniffer Financial Intelligence and Sniffer MultiSegment Analysis – speed application analysis with advanced and specialized packet-flow statistic, charts, and graphs.

Sniffer Intelligence provides several different filtering techniques, including HyperLocks, Multi-Dimensional Views (MDVs) and additional filters, to help focus on different network data. All of these techniques perform the same fundamental task – they limit the data shown in the Intelligence views, winnowing down irrelevant information so that only the data necessary to make a diagnosis is available.

The Sniffer Intelligence filters provide a rich array of criteria for refining the data set, including addresses, applications, measures, Voice over IP (VoIP) phone numbers, Quality of Service values, MPLS labels, conversations, FIX attributes, and VLAN IDs.

Expert Analysis

Sniffer® Intelligence modules provides industry-leading Expert analysis and data mining capabilities for the nGenius InfiniStream family to reconstruct network activities and accelerate diagnosis of performance issues. nGenius InfiniStream appliances store and index network packets in a format that is designed to minimize the time spent sifting through large trace files, while Sniffer Decodes and Expert analysis provide traditional support for hundreds of symptoms and diagnostics. Both features enable users to quickly pinpoint the cause of performance incidents and the preceding conditions.

Flexible Filtering Options

The nGenius InfiniStream appliance's flexible filtering options enable the user to refine the data set – both before and after packet capture – and look at the exact time, user or application associated with the network disturbance. Pre- or post-capture filters can be used to create custom rules to identify the precise combination of addresses, ports, applications and patterns needed to recognized network and security-related events.

Pre- and post-capture filters can be created using any combination of:

- MAC and IP addresses
- TCP or UDP ports
- DNS names
- Protocols
- Hex, binary, or text patterns
- ToS (Type of Service)

Smart Recording and Data Mining

NetScout's Smart Recording and Data Mining (SRDM) technology provides an intelligent data reduction and storage optimization approach that enables organizations to selectively record and store – on a per application basis – all, none, or part of the packets of interest. SRDM extends the amount of data that can be recorded and the length of time that the data is available for retrieval. It can also play an important role in maintaining compliance by limiting who has access to payloads that contain sensitive personal, financial, or medical information.

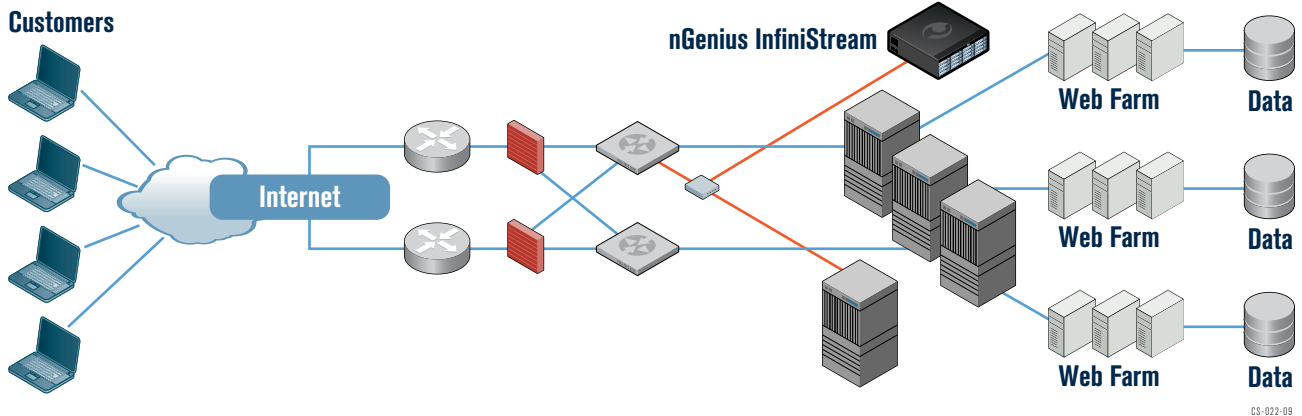


Figure 1: The nGenius InfiniStream was positioned in front of the server farm, an important aggregation point that enabled it to monitor multiple applications.

Case Study: Financial Institution Resolves Elusive Problem with nGenius InfiniStream

In this in-depth, technical illustration, a financial institution used the capabilities of the nGenius InfiniStream appliance to resolve a perplexing intermittent problem that was customer-facing and had cost the company numerous frustrated staff hours. The postmortem analysis revealed that filtering played a key role in several steps of the troubleshooting process and that several types of filtering contributed to its successful resolution, including:

- 1) Pre-capture filters to increase storage retention;
- 2) Time-based filters to overcome unattended monitoring;
- 3) Expert filtering to identify conversations of interest; and
- 4) Post-capture filtering to correlate events and identify root cause

The problem in question was with a web-based financial analysis system that would periodically drop connections, causing customers to have to re-login and lose the account changes they had performed but that the system had not committed. This was a very frustrating experience for some customers who were often working with changes involving thousands of dollars. The business interpreted the impact of the problem not simply as affecting customer service and customer satisfaction, but also as a potential legal risk. Complicating the situation was the fact that the problem only happened about once a week.

Challenge #1: Shared SPAN session and Extending Storage Time

The customer needed to troubleshoot an Internet-based application that used a server switch whose monitoring SPAN session was configured to monitor multiple applications living on multiple VLANs on the same switch (refer to Figure 1). This set

up allowed a signature-based Intrusion Detection System (IDS) to monitor for intrusions and the nGenius InfiniStream appliance to monitor for performance degradations.

Because the problem was only occurring about once a week, the customer wanted to expand their ability to look back in time to view multiple occurrences of the problem. The first step the network staff took was to set up pre-capture filters on the box to capture and store only the desired application traffic and ignore any unneeded traffic (See Figure 2 for a description of the metrics that can be used for filtering). This had the benefit of extending the time information could be stored from two days to three weeks.

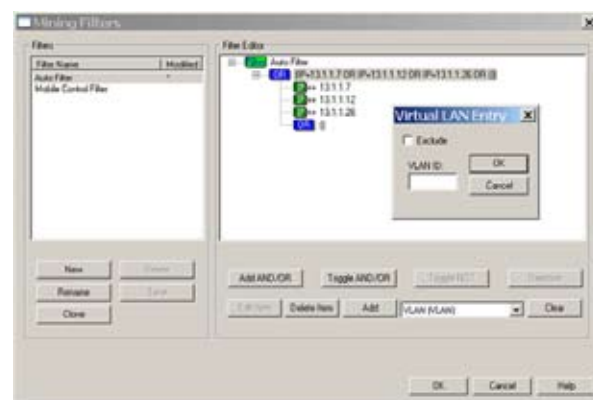


Figure 2: Capture filters can be based on subnets, IP addresses, ports, protocols, MAC addresses or VLANs. Filtering can be combined with frame slicing to further increase the look back capabilities of the product.

Challenge #2: Identifying the Appropriate Packets

With traditional portable analyzers or packet capture technologies, one of the most difficult things to do is filter network traffic based on when the analyzer collected the packets. The chief

Challenge #4: Identifying Extremely Rare Patterns with Post-Capture Filters

The first hypothesis was that the event was triggered from a particular http transaction. Therefore, the customer created a post-capture filter to see packets with HTTP GETs in them (See Figure 5). After some analysis, the engineer could not correlate the performance problems to any particular GET, so he then performed a similar analysis using HTTP POST. This time the engineer was able to determine that POSTs were employed in a seldom-used feature and were the cause of the problem.

Using the absolute time in the decode screen, the engineer was able to identify that immediately before a POST all of the application traffic was healthy with very little anomaly. But immediately following a POST, the particular server receiving the transaction would display the symptoms. The engineer then went back to the event five days previous, re-mined the data and again found that the POST calls were interrupting the performance of the servers that received them. Armed with this information, the engineer turned the issue over to the development staff who quickly discovered that their POST routine had recently been modified with an incorrect script pointer. This erroneous pointer was causing a web server process to lock up and bringing the entire server to an extremely unsteady state. After fixing the pointer file, the application problem was resolved.

Wrap Up

In retrospect, the diagnosis and resolution of this problem were largely based on the ability to successfully record

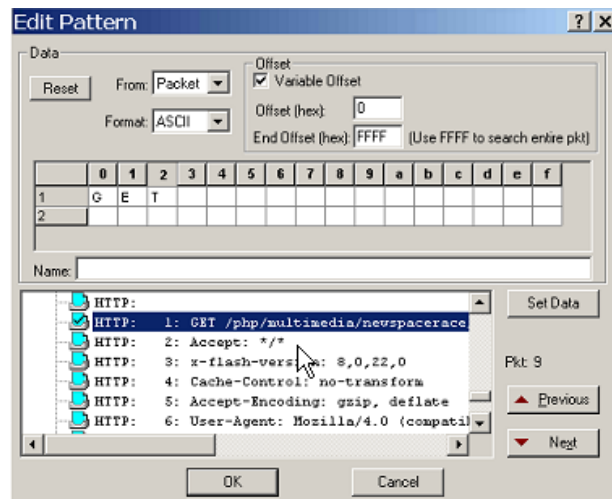


Figure 5: A post-capture filter enabled the customer to view packets containing HTTP GETs and POSTs.

and quickly filter packets to find the appropriate information. With traditional packet capture technology, the buffer wrap time would have been far too small, and searching through the buffer for particular traffic far too time consuming, to consistently diagnose intermittent problems of this ilk. The unique indexing and storage capabilities of nGenius InfiniStream appliances streamline and simplify troubleshooting. By setting pre-capture filters, the engineers extended their ability to look back in time to track a problem that happened approximately once a week. Using time-based mining filters, they were able to quickly isolate suspect traffic occurring during the times their help desk reported the problem. This suspect traffic was analyzed using the Sniffer Intelligence's Expert analysis to identify anomalies and conversations of interest. From here, the diagnosis was made possible by identifying extremely rare patterns using post-capture filters. And finally, after correlating HTTP POSTs

with the beginning of the problem incident, the problem was quickly resolved by providing the right information to the right team to implement the fix.

The end result was that the company was able to successfully eliminate a problem that had been upsetting their customers for several weeks.

Conclusion

The nGenius InfiniStream appliance is an intelligent Deep Packet Capture device that delivers dedicated, 'always on' monitoring and continuous capture capabilities for real-time and back-in-time analysis. Used standalone or as the foundation for the nGenius Service Assurance Solution, the nGenius InfiniStream appliance leverages intelligent Deep Packet Capture (iDPC) technology to analyze the traffic packets traversing the network for rapid problem isolation and service delivery assurance.



Corporate Headquarters

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

European Headquarters

NetScout Systems (UK) Ltd.
100 Pall Mall
London SW1Y 5HP
United Kingdom
Phone: +44 (0)20 7321 5660

Asia/Pacific Headquarters

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

©2009 NetScout Systems, Inc. All rights reserved.

NetScout, the NetScout logo, nGenius, Sniffer, InfiniStream are registered trademarks of NetScout Systems, Inc. Other brands, product names and trademarks are property of their respective owners. NetScout reserves the right, at its sole discretion, to make changes at any time in its technical information and specifications, and service and support programs.