

*Get Real...*

*...Real Solutions For Global Networks*

[www.niksun.com](http://www.niksun.com)

# Managing Enterprise Networks

---

Network Monitoring, Quality of Service  
Management and Intrusion Monitoring



NIKSUN, Inc.  
111 North Center Drive  
North Brunswick, NJ 08092  
P +1.732.821.5000  
F +1.732.821.6000  
E [info@niksun.com](mailto:info@niksun.com)

---

## Highlights

- Overview
- Business Requirements
- The NIKSUN Solution
- NIKSUN - Network Performance & Security Monitoring Solutions
- NIKSUN - Security Monitoring Solution
- NIKSUN Vision
- About NIKSUN

## Overview

Network management challenges today go well beyond simple network availability. Issues like Quality of Service (QoS), Service Level Agreements (SLA), network growth/deployment, and most importantly, network security are all critical areas that require advanced troubleshooting, diagnosis, and management tools. New applications are continually being deployed such as ERP, CRM, and mission critical e-Business services. All of these new applications are driving network management demands from response time issues to network security breaches. Networking professionals are faced with more pressure than anytime previous in their careers. They have less technical staff, “n” times more users, and most importantly, an operational environment with “zero” tolerance for downtime. Today the network is the business. Without an enterprise network running at peak efficiency, business functions in all areas come to a halt.

## Business Requirements

Areas of network management can be clearly defined and segmented. From the Business Management standpoint activities like planning, design, simulation, tuning, and network modeling are required.

Service Management includes base lining network performance, historical usage analysis, SLA reporting, and performance management. In Operations Management the provisioning of fault management, administration, monitoring, inventory, and console tools is critical. Element Management (management of routers, network access devices, etc.) is one of the easiest areas due to the variety and sophistication of element management tools provided by the networking equipment companies.

The challenge networking professionals face is the upper three areas of network management. They can deploy a variety of solutions, each tailored for a specific area of network management. This “pizza box” approach creates a number of challenges from the installation of numerous vendor products to the challenge brought on by maintenance and management of these platforms – none offering an end-to-end seamless solution.

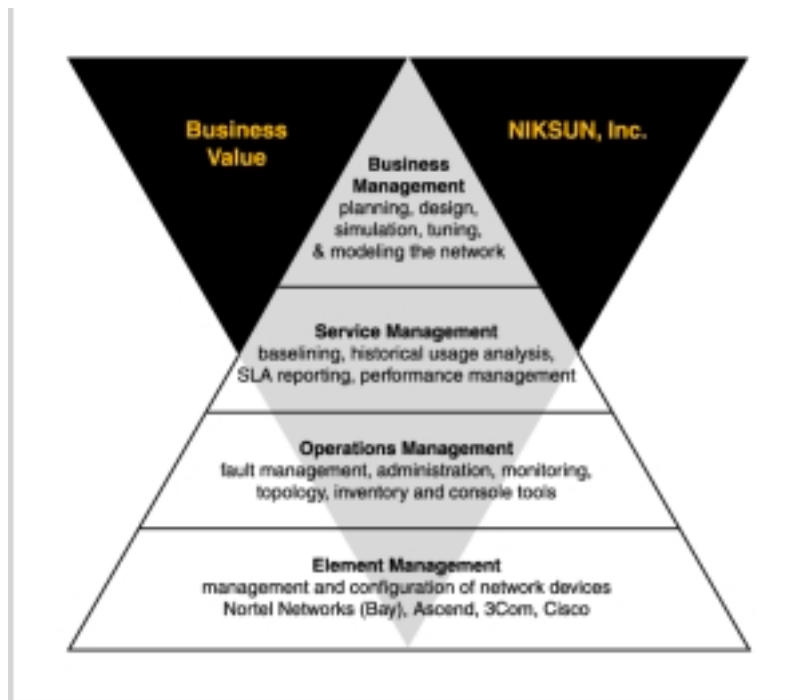


Figure 1 - NIKSUN, Inc. Business Value

## The NIKSUN Solution

### Solution

- Who is using your network?
- How much bandwidth is being used by which users?
- What applications are consuming your bandwidth?
- What was the root cause of the problem?

The NIKSUN approach is to provide a single passive appliance that will meet the Business Management, Service Management, Operations Management, and security requirements of today's largest and most demanding networks. We have designed a scalable system that is based on 11 patent pending technologies that can provide detailed network analysis data on LAN traffic for 10/100 to Gigabit LAN speeds and WAN traffic up to OC-3 today with an architecture goal of OC-192.

When you evaluate your network performance there are a number of questions that need to be asked. Who is using your network? How much bandwidth is being used by which users? This is critical for capacity planning, network architecture, and design. You need to know what applications are consuming your bandwidth. How much Internet, Extranet, e-business, and legacy applications are consuming your network capacity? Evaluate peak loads or network outages. When did they occur? What was the effect on the network segment, application, or user? And most importantly: what was the root cause of the problem? How can I isolate what really happened? From a network management and planning standpoint we need to look at the network and be able to drill down to the network segment and device performance. Is the network

## Data Capture

- Data can be recorded and archived for hours or days
- Detailed post-event analysis
- Troubleshoot in real-time
- Identify the root cause
- Archived proof of violation

causing the application latency or is it a server problem? All of this information is critical to evaluate true network performance.

One of the most powerful features of the NIKSUN solution is our ability to do continuous data capture. Network traffic can be recorded and archived for hours or days. This capability allows for detailed post-event analysis. Imagine having a problem over the weekend and being able to troubleshoot it in real-time on Monday. Imagine the power of viewing a past outage as it is/was occurring. No more guess work. No more installing test equipment with the hope of capturing the problem again. How many times have you chased an intermittent problem for weeks? If you had a network performance problem you can go back and review in detail what was traversing the network. What caused the performance degradation? Was it application based or was a user downloading a large MP3 file off the Internet? Diagnose the problem – identify the root cause – and, if necessary, have archived proof of the cause or violation.

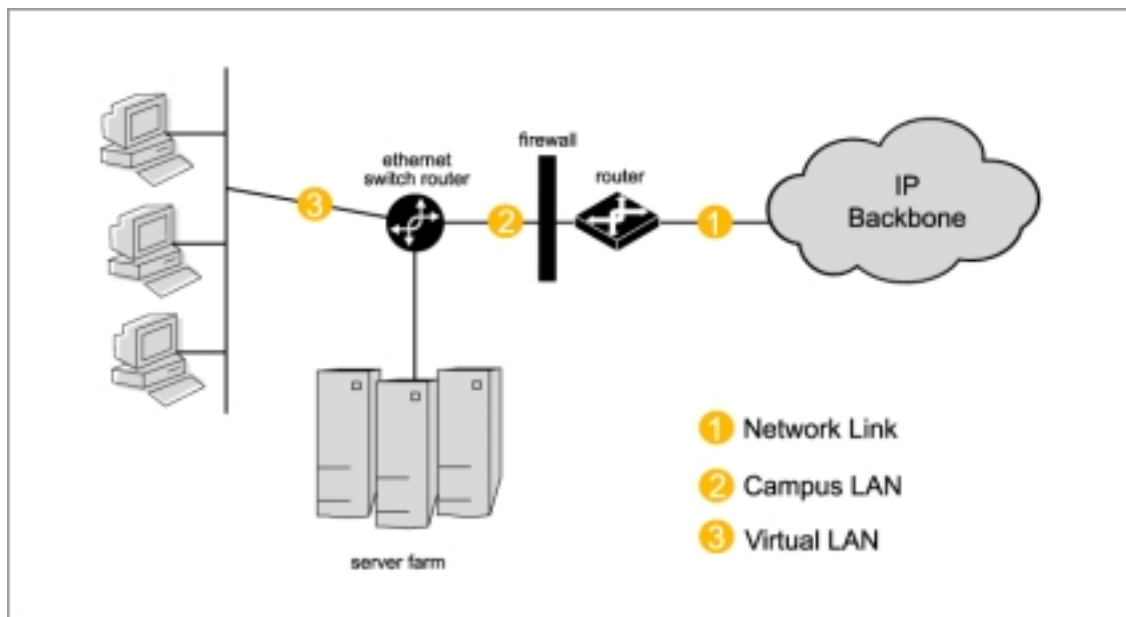


Figure 2 - Typical Network Deployment

## NIKSUN - Network Performance and Security Monitoring Solutions



Figure 3 - Link Level Analytical View

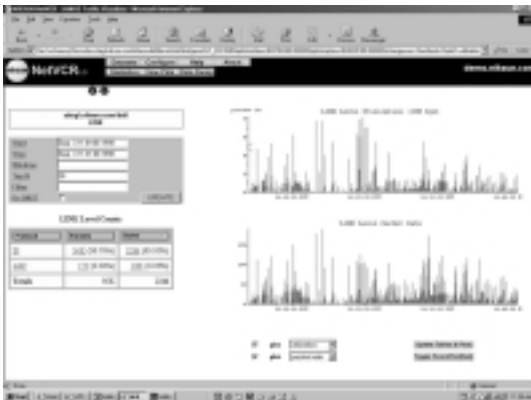


Figure 4 - Filtered Time Specific View

The heart of the NIKSUN technology is our ability to acquire and archive network traffic at the byte level. This data is collected from network access links or network backbones. This information gathering technology handles data in real-time across multiple interfaces. Today we record up to 500 Mbps per second. The real power of our technology is our ability to store and manage large volumes of data – up to terabytes. This data is managed by a proprietary management solution that can be quickly accessed. Standard database technology available today could not manage the data and granularity required for quick analysis.

With our solution you could have a great deal of data stored – let's say three days – and pick a single minute during that time period and within seconds have the detailed data for analysis. You can zoom into any IP source or destination, application, or combination. It is all managed from a very easy to use browser based GUI.

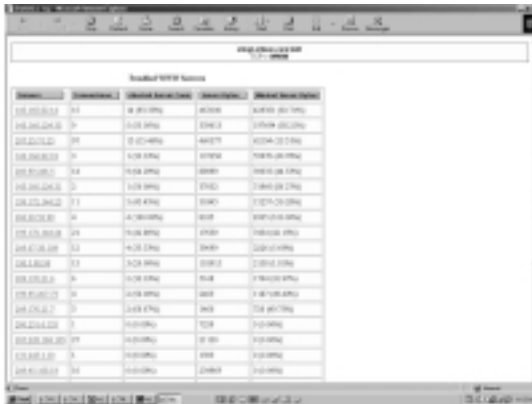
The NIKSUN architecture provides a foundation for future applications. It's modular design architecture permits ease of development of new features and functions with minimal time to market. This enables NIKSUN to be very responsive to the needs of our existing customers and the marketplace. NIKSUN's patented approach sets a new standard for network performance monitoring and management. NIKSUN provides a window into the network for real-time analysis AND records/archives — ALL of the data traffic for post-event analysis.

NIKSUN solutions can be deployed network-wide across multinational networks – it also has the scalability to view the performance down to the application and user level.

NetVCR® provides the ability to do complete traffic analysis on layers 2 to 7. You can view data down to the application layer, device layer, and user layer. This gives you the ability to do inclusive surgical troubleshooting. You can start at the lowest level and surgically troubleshoot the problem – all with an easy to use point and click browser based GUI. This analysis can be done in real-time to solve a current problem, or you can search and troubleshoot in real-time last night's problem or outage. While you are

# Security

- Monitor all traffic
- Complete activity trail if there is a breach
- Identify individuals responsible for network breaches



Timestamp	Client IP	Server IP	Request	Response
08:00:00.00	192.168.1.1	192.168.1.2	GET / HTTP/1.1	200 OK
08:00:00.01	192.168.1.1	192.168.1.2	GET / HTTP/1.1	200 OK
08:00:00.02	192.168.1.1	192.168.1.2	GET / HTTP/1.1	200 OK
08:00:00.03	192.168.1.1	192.168.1.2	GET / HTTP/1.1	200 OK
08:00:00.04	192.168.1.1	192.168.1.2	GET / HTTP/1.1	200 OK
08:00:00.05	192.168.1.1	192.168.1.2	GET / HTTP/1.1	200 OK
08:00:00.06	192.168.1.1	192.168.1.2	GET / HTTP/1.1	200 OK
08:00:00.07	192.168.1.1	192.168.1.2	GET / HTTP/1.1	200 OK
08:00:00.08	192.168.1.1	192.168.1.2	GET / HTTP/1.1	200 OK
08:00:00.09	192.168.1.1	192.168.1.2	GET / HTTP/1.1	200 OK
08:00:00.10	192.168.1.1	192.168.1.2	GET / HTTP/1.1	200 OK
08:00:00.11	192.168.1.1	192.168.1.2	GET / HTTP/1.1	200 OK
08:00:00.12	192.168.1.1	192.168.1.2	GET / HTTP/1.1	200 OK
08:00:00.13	192.168.1.1	192.168.1.2	GET / HTTP/1.1	200 OK
08:00:00.14	192.168.1.1	192.168.1.2	GET / HTTP/1.1	200 OK
08:00:00.15	192.168.1.1	192.168.1.2	GET / HTTP/1.1	200 OK
08:00:00.16	192.168.1.1	192.168.1.2	GET / HTTP/1.1	200 OK
08:00:00.17	192.168.1.1	192.168.1.2	GET / HTTP/1.1	200 OK
08:00:00.18	192.168.1.1	192.168.1.2	GET / HTTP/1.1	200 OK
08:00:00.19	192.168.1.1	192.168.1.2	GET / HTTP/1.1	200 OK
08:00:00.20	192.168.1.1	192.168.1.2	GET / HTTP/1.1	200 OK

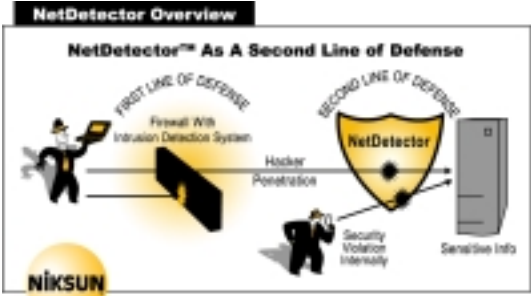
Figure 6 - WWW Server Performance

troubleshooting, the system continues to record current traffic – you never have to stop recording to do troubleshooting. NetVCR can easily diagnose multicast network problems and has the ability to create virtual interfaces that monitor multiple paths, links, or can be grouped by customer or department.

NetVCR provides very valuable statistics – from TCP layer performance including round-trip response times, application/server response times, as well as re-transmission rates. For web-based traffic we provide valuable statistics on user abort rates. These are very valuable statistics that provide information on how many web users are aborting their requests due to poor performance and/or content? How many times have you aborted a request because the web site you went to was congested?

Because we capture all traffic on the links we are recording, we have a great deal of information stored. We utilize easy to use point and click commands that allow you to quickly drill down for host and application performance. You can also set filters to only record a specific data stream – by application, host, or user.

## NIKSUN – Security Monitoring Solution



NetDetector™ provides a second line of defense to firewalls. It monitors all traffic coming through the firewall as well as internal traffic on the LAN. It can detect intrusion schemes such as scanning or Denial of Service attacks. NetDetector generates alarms via JAVA/SNMP that can be sent to network manager systems (i.e., HP Open View or Tivoli). It also can be set up for direct pager notification of a security breach alarm. NetDetector is capturing all data traffic so that in the event of a breach a complete activity trail is available. Byte for byte analysis and playback of network breaches can be viewed. This will allow you to identify and prosecute the individual responsible and establish procedures or systems changes to prevent it in the future.

From an Intranet or Extranet standpoint we can playback historical sessions by user, viewing each transaction just as they traversed the network. You can view screen for screen http pages just as the user did. No other system provides this inclusive level of data capture.

---

## About NIKSUN

- Network performance
- Network monitoring
- Security surveillance
- Forensic analysis
- [www.niksun.com](http://www.niksun.com)

## NIK SUN Vision

Our core technologies of high-speed byte level data capture, recording, and analysis provide a superior foundation for future application development. Today we provide detailed data analysis with NetVCR, plus in-depth and detailed security breach detection and analysis tools with NetDetector. In the future we will be developing extensive tools for easy to use Service Level Agreement management, VoIP, and detailed web analysis tools.

In summary, NIKSUN has developed the only solution that manages both LAN and WAN in the same platform, supporting link speeds up to OC-3 and beyond. Providing detailed data for QoS, SLA, network operations, and network security. All of this plus a real-time network diagnostic and troubleshooting tool in one system. No other system gives you an inclusive audit trail for network analysis. No other solution monitors and records data on a byte for byte level. No other solution has the range of circuit types and speed.

## About NIKSUN

NIK SUN, Inc., headquartered in North Brunswick, New Jersey, is the recognized worldwide leader in developing and deploying network performance, monitoring, security surveillance, and forensic analysis system solutions.

The company's patent pending real-time data analysis and recording technology enables an Enterprise, ASPs, ISPs, and carriers to provide secure and reliable network infrastructures and services. NIKSUN's family of products are the only network appliances that continuously capture and analyze LAN, MAN, and WAN traffic at up to Gigabit rates in a single platform.

NIK SUN has research and development facilities in New Jersey, Silicon Valley, and India, and many members of the NIKSUN team have extensive background with the Bell System and other industry leading institutions. The company has sales offices in major cities throughout the U.S. and Europe, as well as partnerships with industry leading network solution providers worldwide.

*Get Real...*

---

*...Real Solutions For Global Networks*



NIKSUN, Inc.  
111 North Center Drive  
North Brunswick, NJ 08092  
P +1.732.821.5000  
F +1.732.821.6000  
E info@niksun.com

[www.niksun.com](http://www.niksun.com)