NIKSUN Wins InfoWorld's
2006 Technology of the Year Award
NIKSUN NetVCR: Best Network Analysis Tool

InfoWorld®

April 4, 2005 ■ Issue 14

GET TECHNOLOGY RIGHT®

NETWORKING

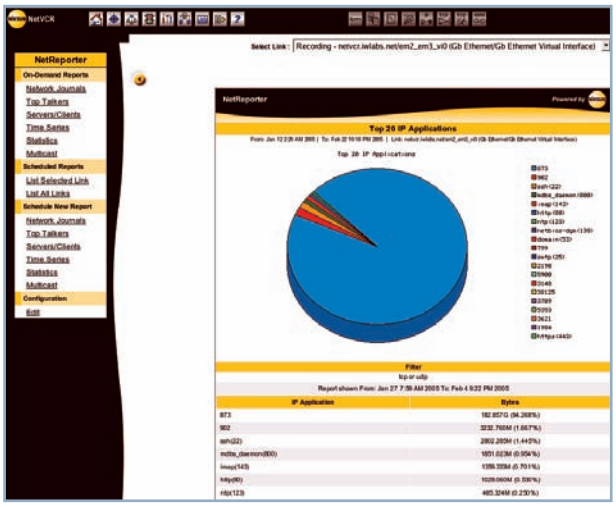
Niksun Boosts the Protocol Analysis Bar

NetVCR is a network admin's dream: It sees, stores every bit of enterprise network activity

IT'S ONE THING TO implement a network protocol analyzer on a segment to determine traffic patterns and utilization; it's quite another to perform these functions and to capture and store every bit seen on the wire.

Niksun's NetVCR 2005 does exactly this, thanks to its embedded database. Think of it as a protocol analyzer that never forgets.

Niksun's product line consists of several integrated components that perform various duties related to network forensics, security, monitoring, and reporting. NetVCR is available as a stand-alone or integrated solution; I tested it as it would be deployed in stand-alone fashion on an enterprise network.



NetVCR records all packets on the wire and provides instant analysis of the data; this report shows the top 20 apps seen in a specific time period.

Rare Flexibility

The NetVCR is built on a Supermicro server chassis, with dual 2.8GHz P4 Xeon CPUs, 2GB of RAM, and a configurable storage layout. My review unit came with 530GB of storage in a RAID5 SCSI array.

The server runs FreeBSD with a custom kernel. Console interaction with the device is limited to the initial setup, as the solution is completely Web-driven.

Configuring the unit was very simple; an initialization script — accessed via a standard KVM or serial connection — handles all network parameters and prepares the box for deployment. Following that, all access to the appliance is through a Java application served up via the Web.

The only problem I had was that the default log-in specified in the manual didn't match the appliance, but an e-mail to Niksun got me the correct log-in, as well as a pointer to a custom executable in the OS that resets the Web password. There is no relation between the Unix passwd file and the Web front end.

The NetVCR is available with a wide variety of network interfaces, including 10/100 copper Ethernet, gigabit copper or fiber

Niksun NetVCR 2005

Niksun niksun.com

EXCELLENT 8.8

Ease-of-use (25%)	8
Manageability (25%)	9
Performance (15%)	9
Setup (15%)	9
Scalability (10%)	9
Value (10%)	9

COST: $30,000 and up, depending on licensed modules

BOTTOM LINE: With network performance trending, SLA/QoS monitoring, alerting, and broad reporting tools, Niksun NetVCR 2005 proved to be a complete network-analysis package. Additional modules are available to handle VoIP traffic and more. If you need to know everything about your network, this is a great solution.

Ethernet, HSSI (High-Speed Serial Interface), ATM, Packet over SONet, T1, T3, OC3, OC12, and more, including multilink PPP, ISL (Inter-Switch Link), and 802.1q support. With such a wide range of interfaces, the NetVCR solution can be placed on almost any type of network, anywhere in the datacenter.

That kind of flexibility is rare and very valuable. My review unit came with a gigabit fiber monitoring interface, and I placed the NetVCR on a gigabit fiber port on a Dell PowerConnect 5524 gigabit switch. I then mirrored all ports on that switch to that fiber port. This isn't the ideal placement, but I didn't have a full-duplex gigabit fiber network tap to use. (In a production environment, use of a full-duplex tap is recommended.)

Nevertheless, I immediately saw network flows appear on the NetVCR Web interface. The interface is driven via a Java applet and is a good blend of function and style without being too cluttered. That said, there are a lot of functions available, and initial navigation through the interface is slightly daunting. After you get comfortable with the GUI presentation, however, it's easy to get to the data you need.

Delving Into Data

As data comes across the wire, the NetVCR catalogs and organizes the packets into the internal database. This database is proprietary to Niksun and uses as much of the available space on the appliance as possible. NetVCR sees data sets within the Web interface as interfaces, whether physical interfaces or time segments of captured data. This convention allows for easy data mining within the appliance and is simple to manage.

After I had the appliance up and running for an extended length of time, I began configuring automated reports. In approximately 15 minutes, I set up the NetVCR to e-mail me nightly network traffic reports, with graphs and data on everything from the top protocols in use and the top host interactions, to the busiest and slowest servers measured by average response time.

Reporting data choices are extensive, but the interface to configure reporting options suffers slightly due to the vast amount of available report elements. The reports are produced in a wide variety of formats, from raw graphs to nicely organized PDF, HTML, and CSV (comma-separated value) files.

I chose a PDF report, which was well laid out and provided quick, direct links from the table of contents to the relevant data. For instance, the busiest-servers section shows a bar graph of the servers carrying the heaviest load as determined by the number of connections, plus a breakdown of each server's load by protocol. Below the graph is the raw data, showing each server by IP and DNS name, as well as each protocol and the number of connections seen.

All the reports can be passed through BPF (Berkeley Packet Filter) strings to weed out potentially useless data. This capability comes in very handy, as it allows an administrator to create custom reports that first focus on potentially problematic network segments or hosts and then show only the data relevant to that specific entity. When trying to determine the cause of intermittent network problems, this is a powerful tool.

Analysis Made Easy

Because the NetVCR captures and stores all the packets seen on the wire, you get easy, complete access to historical data. Beyond the reporting capabilities of the NetVCR, it's possible to select date ranges of stored data and pass them to low-level protocol analyzers, such as Ethereal, for deep packet inspection. (Ethereal is embedded into the UI, so no data export/import is necessary.)

The limit of data captured is determined solely by the available storage, and it's possible to attach a NetVCR to a SAN array for extended storage capacity. Plus, Niksun takes the NetVCR beyond protocol analysis by implementing options packages as simple add-ons. In this manner, you can gather specific data on network applications such as VoIP.

Overall, the NetVCR is the most powerful network analysis tool I've seen. The scope of the reporting and analysis engines within the UI is broad, and the data it collects is quite useful. If you need to know everything about your network, take a good look at the NetVCR.

— *Paul Venezia*