NetDetector™
The Most Advanced Network Security and Forensics Analysis System
Introduction

Every system attached to the Internet is a potential candidate for a malicious attack. Even the most secure Internet sites, corporations, and government agencies have experienced security violations and network attacks. To deal with those risks, organizations are investing resources into increasing the security of their networks. However, completely preventing security breaches appears to be unrealistic at present.

This white paper provides an in-depth description of how NIKSUN’s premier network security system aids in maintaining a secure network by providing organizations with the proper tool to detect and recover from security breaches. NIKSUN’s NetDetector is an affordable, non-intrusive, high-speed network surveillance appliance, analogous to a security camera for the network. The NetDetector system enables organizations to easily perform forensic analysis on network events and network intrusions.

NetDetector continuously records all of the traffic on the networks to which it is connected. While traffic is being recorded, NetDetector simultaneously analyzes the captured data to detect traffic anomalies and immediately provides alerts when certain thresholds are exceeded. These thresholds are user programmable, and when met, the high-speed Mercury engine of NetDetector ensures continuous capture/storage and analysis/alert without missing a packet, stream, or flow on the network. The alerts provided by NetDetector can be in the form of a pop-up screen, email, short text message to cell phone/pager, or an SNMP trap.

NetDetector does not actively poll other devices on the network. NetDetector captures traffic directly from the network through non-intrusive taps, and creates a large database from captured traffic and associated statistics. This database can be easily queried for post-event analysis, which significantly reduces the time required to determine how an intrusion occurred.

A Three-Tier Approach to Network Security

With increased connectivity, more systems are subject to unauthorized access and attacks. In today’s environment, organizations are taking a three-tier security approach to protect their networks and information.

<table>
<thead>
<tr>
<th>Three-Tier Security Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Avoidance</strong></td>
</tr>
<tr>
<td><strong>Intrusion Detection</strong></td>
</tr>
<tr>
<td><strong>Security Investigation</strong></td>
</tr>
</tbody>
</table>
Network security starts by having the proper protection to avoid security breaches and ends by having the appropriate investigative tools to be able to restore the network to a secure state once the security breach has occurred.

The NIKSUN NetDetector product addresses the detection and investigation tier of the network security model. NIKSUN’s non-intrusive technology enables anomaly detection, and data capture and analysis for network security investigation (also known as network forensics). NIKSUN believes that these two capabilities are critical for establishing and maintaining secure computing environments.

This white paper provides an overview of how NetDetector complements current intrusion detection systems and provides the information required to perform investigation of security incidents.

**Intrusion Detection and NetDetector**

Every system attached to the Internet is a potential candidate for a malicious attack. Organizations can detect most network attacks by deploying intrusion detection systems. By definition, intrusion detection systems (IDS) are tools that collect information, analyze that information for patterns reflecting misuse or unusual activity, and report the outcome of the detection process.1

Intrusion detection techniques can be classified into signature-based detection and anomaly detection. Signature-based intrusion detection uses patterns of well-known attacks or weak spots of the system to identify intrusions. However, if one uses more than a handful of signatures for detection by IDS systems, their capacity to handle traffic drops dramatically i.e., can be as low as 20-30 Mbps on a 100 Mbps FE link. Anomaly detection tries to determine whether deviation from the established normal usage patterns can be flagged as intrusions. Most commercially available intrusion detection systems are signature-based.

NetDetector complements signature-based intrusion detection systems with very powerful anomaly detection capabilities. Security administrators are able to define alerts based on baselined “normal” traffic conditions, and NetDetector will inform the security administrator when the traffic recorded exceeds the defined thresholds.

NetDetector can detect network attacks in-progress by analyzing traffic flows and traffic patterns. The attacks detected include excessive traffic loads, resonance and probing attacks, denial of service attacks, and IP address spoofing.

Most intrusion detection systems exhibit a high false positive rate. NetDetector can help the security administrator in analyzing these alerts to determine whether the alert is real. In addition, intrusion detection systems have difficulty detecting attacks that are spread out over time or locations; attack methods that are becoming more common. They are not able to keep up with state information over a long period of time and match all the data.

---

1 Rebecca Bace, “An Introduction to Intrusion Detection and Assessment”, ICSA White Paper
Investigation tool to analyze and recover from security breaches

Need to record all network traffic for post-event investigation

Complete audit trail helps understand attacks and prevent/detect future attacks

Non-detectable recording and analysis engine for evidence gathering

together to detect attacks spread over long-periods (i.e., most IDS do not detect a scan when the intruder is probing the network every 15 minutes). Due to its large buffer space, NetDetector is able to detect slow scans. In order to detect a slow scan, security administrators need to analyze all traffic for an extended long window (i.e., 24 hours). In that interval, there are enough probing packets in the traffic to differentiate them from the regular traffic.

Security Investigation and NetDetector

Security administrators cannot rely exclusively on intrusion detection systems for protecting their networks. Even the most secure networks will experience security breaches and unauthorized access. The security administrators need to have the proper investigation and auditing tools to perform a complete post-event investigation and to recover from security breaches.

Security investigation of network events, also referred to as network forensics, is fundamentally different from intrusion detection. Network forensics denotes the ability to re-construct events using a system that records all traffic activity on the network. Network forensics tools are traffic recording and analysis engines that act like the network equivalent of a security camera in a bank. Investigators can go back in time and perform historical analyses of events that have occurred in the past.

NetDetector provides security administrators with complete network forensics capabilities. Security investigations of network events using NetDetector will occur very rapidly. NetDetector allows the network administrator to “look back” in time to fully comprehend the methodology of the attack. By enabling the network administrator to understand the attack, a proper defense can be implemented. Additionally, because NetDetector provides a replay capability, the site now has the ability to test the newly implemented counter-measures by replaying the previously successful attack against the newly implemented defenses.

NetDetector will shorten the lifespan of a new vulnerability by allowing security experts to quickly determine “how” an attack occurred, by providing the packet level information necessary to develop the detection signature and by making the detailed attack information available to develop the patch against future attacks. Without a network forensics tool, reverse-engineering the attack is almost impossible.

Not looking at everything might allow a hacker to slip through without being detected; not recording every packet may overlook key information. To perform a forensic analysis of a security breach, one needs as much data as possible from which to determine what happened. Ideally, one has recorded every single packet that crossed the network during the time of the security breach.

Most hackers learn how to cover their tracks by tampering with audit trails, thus limiting the effectiveness of after the fact analysis on audit logs. Therefore, any forensic tools that are based on log analysis can often miss an attack on the network. However, hackers cannot detect non-intrusive network forensics tools, such as NetDetector, and the data recorded will be maintained out of the reach of hackers.
NetDetector – The Most Powerful Network Security and Forensics Tool

NetDetector is a powerful network surveillance appliance for IP networks. It provides non-intrusive, continuous traffic recording, and real-time traffic analysis of LAN and WAN networks. NetDetector makes continuous copies of data from the network, accurately timestamps the recorded data, analyzes every packet, detects the activities of intruders, sets alarms for real-time alerting, and gathers evidence for post-event analysis and legal prosecution.

NetDetector has been designed and optimized to record traffic at very high rates and analyze the traffic in real-time. NetDetector runs simultaneous processes for data recording, data processing, alert detection, data analysis, and data exporting.

NetDetector provides network administrators with the ability to record large amounts of traffic (hundreds of gigabytes). Once the network traffic has been recorded, users can query the data in any way they desire. NetDetector provides flexible query architecture and an intuitive Web GUI to visualize the traffic and perform complex traffic analysis. By providing complete post-event analysis and application reconstruction capabilities, NetDetector becomes a very effective means to carry out network security and event investigation.

Figure 1 - Typical NetDetector development monitoring a full-duplex Fast Ethernet communication (200 Mbps)
NetDetector – The Ultimate Security Appliance that Captures Everything

NetDetector provides administrators with the ability to perform very complex analyses of the recorded traffic for real-time alerting and post-event security investigation. These capabilities have proven to be very effective at identifying, investigating, and closing security breaches in IP networks.

Real-time Alerting

NetDetector detects host scans, ping sweeps, port scans, and common reconnaissance scans that involve a host sending packets to find out which machines or which services are ‘alive’. NetDetector, with its high-performance statistical analysis engine, is able to identify scan attacks, including very slow scans.

There are a large number of attacks that take advantage of the ability to spoof source IP addresses. NetDetector allows users to create alerts for invalid IP address on unidirectional links, enabling them to detect IP address spoofing very effectively.

NetDetector can be customized to detect other traffic patterns that reflect abnormal traffic behavior. Security administrators can take advantage of the traffic analysis functionality to baseline the network and then define the alerts that they wish to receive.

Post-event Network Security Investigation

NetDetector allows security administrators to visualize large amounts of network traffic, drill down into specific time intervals, filter on specific traffic, and perform complete application reconstruction. The screens presented in this white paper are based on actual traffic from a real network intrusion that occurred at a well-known university.

With NetDetector, a security administrator starts the event investigation by drilling down into the appropriate time interval, applications, and hosts using the Traffic Analysis screen (see Figure 2). The Traffic Analysis screen visualizes the traffic and displays the appropriate tables that allow administrators to filter on the relevant traffic.

If the security investigation involves TCP traffic, the security administrator could then display all the TCP sessions associated with the interval and the appropriate traffic filter. Figure 3 shows all TCP flows that the hacker and the compromised machine were engaged in during the security breach. This screen clearly illustrates the sequential progression of actions that the attacker took to compromise the host.
To continue with the investigation, the security administrator then could reassemble the application data associated with each TCP flow for a very granular investigation. Figures 4 and 5 display the reconstruction of two TCP sessions that were critical in determining the actions taken by the hacker.

Since NetDetector stores all the traffic, security administrators could also display the content of each packet on the Packet Dump screen. Figure 6 displays the two packets used by a hacker to break in into a host using the buffer overflow vulnerability on the sunrpc service.

NIKSUN - Summary

Our core technologies of high-speed byte packet, and session-level data capture, recording, and analysis provide a superior foundation for future application development. Today, we provide detailed quality-of-service analysis with NetVCR® and in-depth, 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.

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 Gigabit Ethernet and that provides detailed data for QoS, SLA, 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 network interface types and speeds.

About NIKSUN

NIKSUN is the recognized worldwide leader in developing and deploying a complete range of network performance monitoring, security surveillance and forensic analysis tools serving a wide range of protocols and interfaces, ranging from Ethernet and Gigabit Ethernet to OC-3. Our family of products are the only network appliances that continuously capture and analyze LAN, MAN and WAN traffic at Gigabit rates in a single platform.

NIKSUN’s product line delivers unprecedented flexibility, scalability and real-time response. The company’s patent-pending real-time data analysis and recording technology enables Enterprises, ASPs, ISPs and Carriers to provide secure and reliable network infrastructures and services.

NIKSUN has facilities in New Jersey, California and India, and sales offices in major cities throughout the U.S., Europe and Asia Pacific. In addition, NIKSUN has developed partnerships with industry leading network solution providers worldwide.
Get Real...

...Real Solutions For Global Networks