INTEGRATED NETWORK MONITORING WITH JUNIPER NETWORKS AND NIKSUN

Protect your network with comprehensive and actionable cybersecurity forensics for in-depth analysis, application reconstruction, and proactive discovery

Challenge

The threat of cyber attack is real. Traditional approaches such as firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) have clearly proven not to provide sufficient protection to address these serious threats.

Solution

Juniper Networks EX Series Ethernet Switches deployed in conjunction with NIKSUN NetDetector/ NetDetectorLive appliances can protect enterprise networks from a wide variety of unknown cyber attacks, unauthorized data exfiltration, and espionage threats.

Benefits

- Provides users with NIKSUN's state-of-the-art technology to simultaneously capture, inspect, mine, correlate, and store everything traversing the network at rates up to 20 Gbps
- Enables drill down to packet-level information for granular forensic analysis
- Supports lawful intercept and Communications Assistance for Law Enforcement (CALEA)
- Includes powerful GUI Web interface console

In today's complicated world of interconnected global computer networks, cybersecurity attacks have become commonplace and far more damaging. Even the smallest of hacks to an enterprise network can result in a public relations nightmare, not to mention causing millions or even billions of dollars in damage, lost revenue, and cleanup costs. Not surprisingly, the actual damage from cyber attacks is far greater than reported according to the FBI. "Stopping terrorists is the number one priority," said FBI director Robert Mueller. "But down the road, the cyber threat will be the number one threat to the country. I do not think today it is necessarily [the] number one threat, but it will be tomorrow." director Mueller continued, "There are only two kinds of companies: Those that have been hacked, and those that will be."

Businesses need to protect their infrastructure and assets from the inherent risk of hacking, espionage, and data exfiltration. NIKSUN provides advanced forensic tools that inform users of security breaches and attacks as they occur. The ability to quickly answer critical questions such as how a breach occurred, what data was exfiltrated, what was comprised, who was affected, why it occurred, and how corrective measures can be initiated is vital to organizational health.

The Challenge

Defending against cyber threats has become increasingly challenging. Unfortunately, no network security product can prevent every criminal or malicious act. Even the most secure government agencies and corporate enterprises have experienced hacking and cyber attacks. Are you prepared if you are targeted, and are you equipped to perform post breach analysis?

The Juniper Networks-NIKSUN Integrated Network Monitoring and Forensics Solution

The NIKSUN cybersecurity NetDetector and NetDetectorLive appliances complement Juniper Networks® IDP Series Intrusion Detection and Prevention Appliances by augmenting a signature-based security solution. NIKSUN appliances provide increased network visibility by capturing and storing all packet data, providing the ability to analyze, inspect, and correlate all data traversing the network at multi-gigabit rates. The joint Juniper and NIKSUN solution provides a best-in-class approach for cyber intrusion, prevention, and advanced network forensic capabilities.

Features and Benefits

NIKSUN NetDetector

NIKSUN NetDetector is a full featured appliance for network security monitoring. It defends against malware, advanced persistent threats (APTs), and botnets by combining anomaly and signature detection with botnet command and control examination and geo IP location threat intelligence. In addition, it offers the deepest and fastest data mining forensics with full application reconstruction and packet-level decodes, at full network line speeds.

Its unique passive approach makes it the ultimate compliment to any existing traditional security architecture such as firewalls, IPS, and IDS. NIKSUN makes sure that you are prepared to know what is happening on your network, if a loss or hack has occurred, and that you have the effective tools for post breach analysis.

NIKSUN NetDetectorLive

NIKSUN NetDetectorLive is designed to provide real-time surveillance over IP networks. Similar to NetDetector, it has the capability to monitor all data flowing across the network and also inspects content, providing visibility and control over how vulnerabilities are exploited or how sensitive/confidential information is being breached. NetDetectorLive creates rich metadata on the fly on all content for easy search and inspection, from minutes to years after an event. The special metadata, along with content categorization, allows for superfast search and reconstruction of events, monitoring the contents of events, as well as accurate and simplified analysis into the complete activity of criminal or subversive organizations.

NIKSUN NetOmni

The NIKSUN NetOmni Alpine provides real-time network-wide data aggregation, analytics, and reporting. Through a single console integrated with NIKSUN appliances throughout the enterprise, it consolidates IDS, forensics, packet capture, flow and SNMP analysis, VoIP monitoring, and other capabilities into a single, unified platform, reducing the IT footprint.

Juniper Networks EX Series Ethernet Switches

EX Series switches enable businesses to deploy a high-performance network infrastructure based on three key tenets: operational simplicity, carrier-class reliability, and integration and consolidation. Working together, these attributes enable the EX Series to deliver ubiquitous access to strategic business assets, reduce network downtime, and enhance overall security to shared access across the extended enterprise.

The EX Series switches provide an open platform for innovation through a modular code base and single release train that enables management partners such as NIKSUN to quickly and efficiently establish interoperability with Juniper solutions.

Summary—NIKSUN and Juniper Join Forces to Make Integrated Network Monitoring and Forensics a Reality

EX Series Ethernet Switches enable NIKSUN NetDetector and NetOmni customers to rapidly deploy and manage a secure switching infrastructure with ease, reducing risk posture while protecting existing investments in their security management platform.

Next Steps

For further information, a product demonstration, or proof of concept (POC) request, please e-mail us at **info@niksun.com** or call 609-936-9999.

For more information about Juniper Networks EX Series switches, please visit **www.juniper.net/us/en/products-services/switching**.

About NIKSUN

NIKSUN is the recognized worldwide leader in making the unknown known. NIKSUN's award-winning appliances deliver unprecedented flexibility and packet capture power. The company's real-time analysis and recording technology is the industry's most comprehensive solution for secure and reliable network infrastructure and services. NIKSUN's solutions are deployed with more than 1,000 enterprise customers, including Fortune 500 firms in over 30 countries spanning large multi-national companies, governments and intelligence agencies, service providers, and financial services companies. For more information, visit our website at **www.niksun.com**.

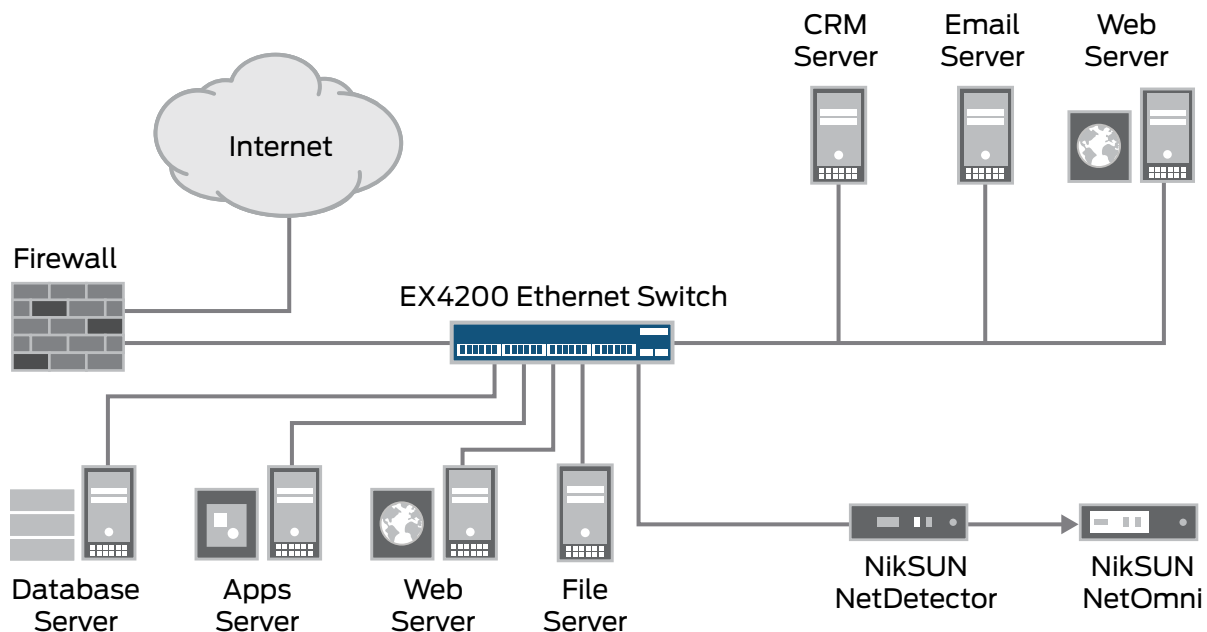# Best-in-Class Approach for Cyber Intrusion, Prevention and Advanced Network Forensic Capabilities

Figure 1. NIKSUN and Juniper Networks joint network monitoring and forensics solution

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at **www.juniper.net**.

3510462-001-EN June 2012   ♻ Printed on recycled paper