

Advanced Intrusion Detection & Prevention

NetKeeper 5105 Series



- **Anti - Intrusion**
- **Anti - DoS / DDoS**
- **Anti - P2P**
- **Anti - Instant Messenger**
- **Anti - Web Post**
- **Worm Mitigation**

NetKeeper 5100 Series

Intrusion Detection and Prevention System

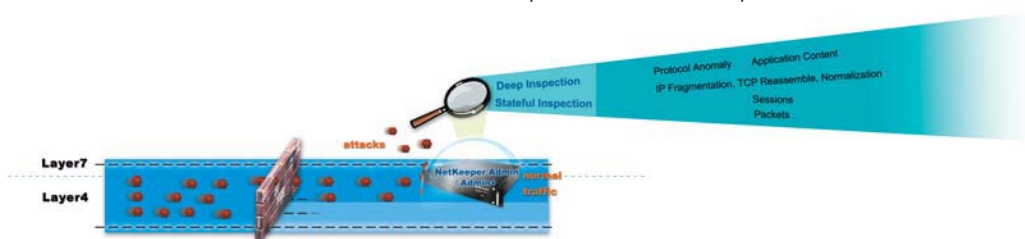
Multiple Functioning Prevention Systems

- ▶ The NetKeeper 5100 series IPS device from BroadWeb Corp. is capable of providing a total protection mechanism against intruders, hackers, and the rapid emergence of new vulnerabilities. The NetKeeper 5100 series encapsulates the world's most technologically advanced, best-of-breed IPS solutions to satisfy all of the business entities, educational facilities and governmental agencies. This ASIC-based intrusion prevention system, with intelligent and "pro-active" blocking and filtering against the most ubiquitous cyber attacks, is dedicated to manage HTTP worms, DoS/DDoS attacks, protocol and traffic anomalies, SYN Flooding attacks in real-time. Its feature-rich functionalities may well improve the productivity of employees and also increase the effectiveness of bandwidth usage within a corporation.

Deep Packet Inspection

- ▶ Based on the fact that traditional firewalls are incapable of inspecting packet contents above layer 4 on a standard OSI structure, intruders and malicious activities attempting to cripple any given business operations can be accomplished fairly easily. Between the increasing scale of assaults by hackers and the ever growing rate of vulnerabilities, firewalls are simply unable to maintain the sophisticated level of protection while allowing legitimate business operations to be transmitted unhindered.

Equipped with Deep Packet Inspection, the NetKeeper 5100 series is the world's only Intrusion Prevention System that is capable of providing any business networking infrastructures with completed protection against both network-level and application-level attacks. Completed protection requires that 100% of legitimate transactions to reach their destination with no discernable impact on network latency even when under severe attack.



Multi-detection Technique

- ▶ The NetKeeper 5100 series incorporates multi-detection technique which is composed of mainly: advanced network anomaly behavior analysis, anomaly packet analysis and multi-detection matching techniques for the purpose of verification on attacking signatures. Based on this impeccably advanced technology, the NetKeeper 5100 series is able to ensure multiple layers of security even under heavy attacks.

Real-time Response to the Attack

- ▶ The NetKeeper 5100 series actively secures the Intranet. According to different security policies, it blocks and drops any illegal connection encountered, reacts to the attack, and informs the network administrator through all possible ways that's being implemented in order to elaborate effective processes of protection.

Logs and Analyzes All Intrusion Events Completely

- ▶ NetKeeper 5100 series logs detailed attack events and proceeds to intercept the packets based upon the pre-set security policies. These network security event logs allow the network administrators to trace attack sources, targets IP addresses, connection ports and communication protocols.

High Availability Support

- ▶ Support Active - Active, Active - Passive High Availability System.

BEMS (BroadWeb Extensible Management System)

- ▶ BEMS (BroadWeb Extensible Management System) is a Java-based central management program that is designed to manage multiple NetKeeper 5100 series appliances at the same time. Integrating with Plugins, BEMS provides user-friendly interface to monitor the real-time network traffics, real-time security-events, and allow users to modify policies and even define their own policies.

Easy-to-use and Query-on-demand Reporting

- ▶ BEMS also makes it easy to manage tasks of report inquiries, such as top-30 intrusion events, attackers, and victims. All of the daily, weekly and regular reports can be printed and sent out in the CVS or HTML formats. In addition, users can use standard SQL commands to generate their own special query reports.

Powered by BSST (Broadweb Security Service Team)

- ▶ BSST (BroadWeb Security Service Team) teams up with a group of network security experts to provide continuous security update for NetKeeper 5100 series. They are committed to study the latest hacking exploits and vulnerability reports over Internet communities. With this knowledge they define the latest defensive policies and provide clients the continuous security. BSST will provide continuous security update for NetKeeper 5100 series, publishing weekly security alerts, network security consultation and technical supports.

Mirror Function

- ▶ NetKeeper 5100 series support port mirror function allowing administrator to view traffic on the IPS ports for diagnostic purpose.

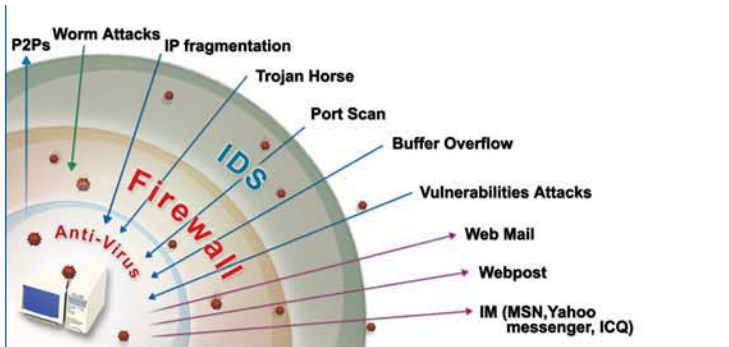
Signature Database

- Multiple string match
- Back Door program detection
- Trojan Horse program detection
- Shellcode detection
- User definable pattern

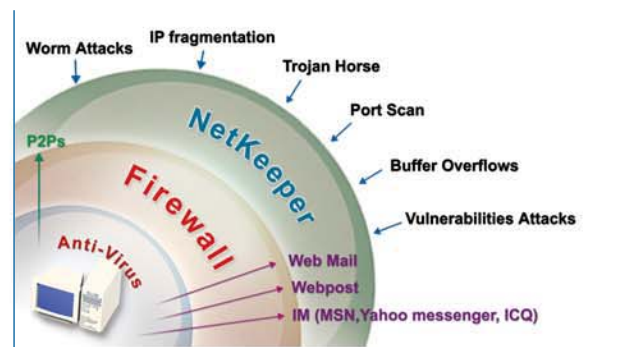
Anomaly Behavior Database

- Statistic Anomaly Detection
- DoS / DDoS Detection
- Flood Detection
- Protocol Anomaly Detection
- SYN flood protection
- Port Scan Anomaly Detection
- BAD TCP state
- IP Sweep detection

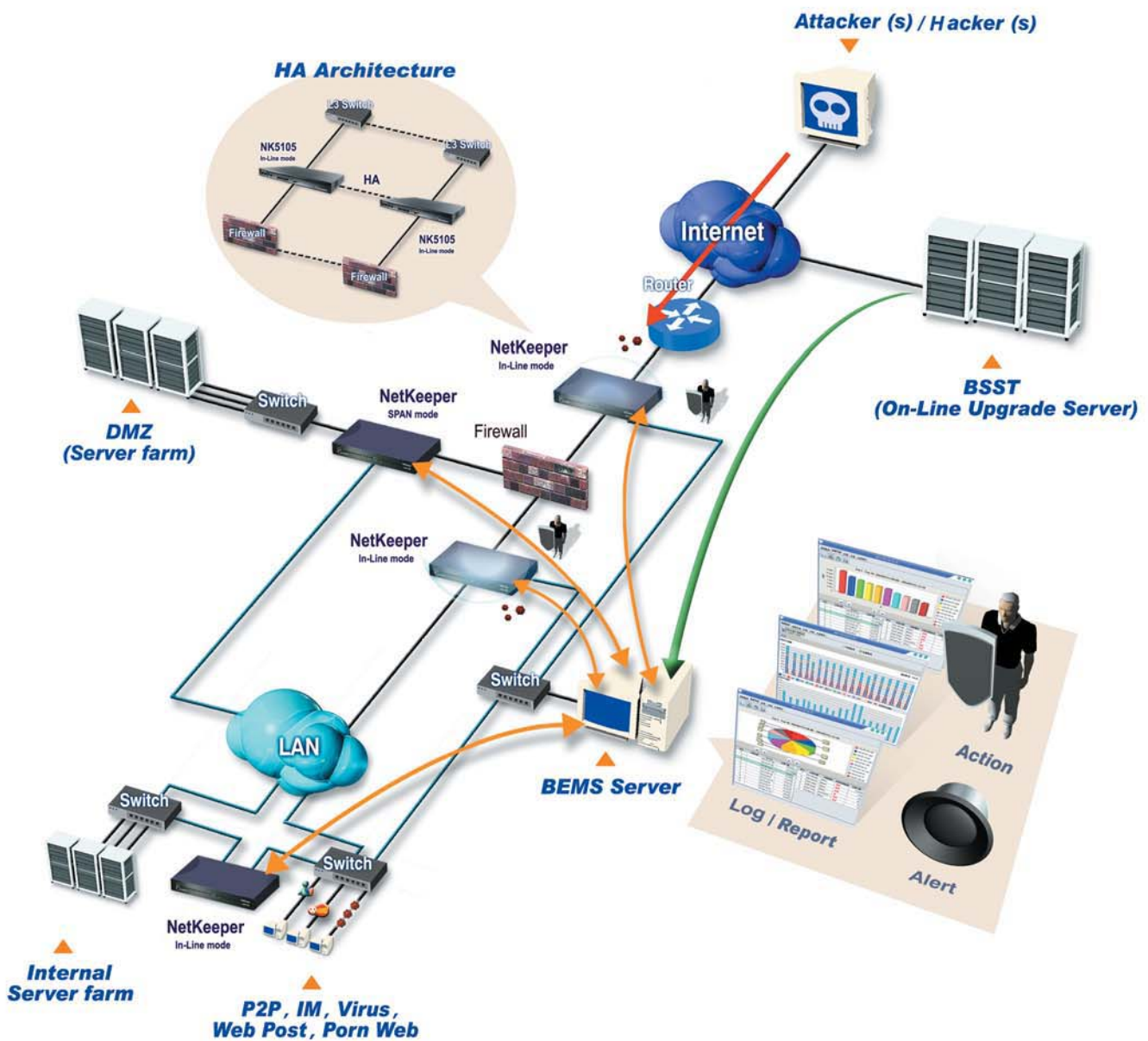
NetKeeper 5100 Series VS. Firewall / Anti-Virus / IDS



Firewall / anti-virus programs cannot provide protection effectively



NetKeeper provides complete protection



Anti-Evasion

- TCP Segment Reassembly
- ADM Mutation (Shellcode Evasion)
- FTP Bounce
- FTP command with Telnet opcode inserted

- RPC fragmentation detection
- Back Orifice detection
- IP fragment reassembly

High Availability (HA)

- Active-Active
- Active-Passive



NetKeeper 5100
Advanced Intrusion Detection & Prevention

NK 5100 software specification

- IPS performance: 1.0 Gbps
- Supports multiple modes of network operation
 - *In-Line*
 - *Tap*
 - *SPAN*
 - *Monitor*
 - *Bypass*
- Contains more than 2,300 signatures , including
 - *Anti-Intrusion*
 - *Anti-DoS / DDoS*
 - *Anti-P2P*
 - *Anti-Instant Messenger*
 - *Anti-Web Post*
 - *Worm Mitigation*
- Highly Secure Embedded Real-Time OS
 - *Supports Stealth mode*
 - *Supports SNMP v2*
 - *Support Unlimited VLAN tagging*
- Multi-detection engine that combines Misuse and Anomaly detection technologies
- Detects anomaly behaviors using multiple detection methods, including protocol and traffic anomaly detections
- Actively detect and block IP/TCP/UDP packet with malicious intrusions and ensure normal network accesses
- Configurable threshold parameters to fit into different network environment
- User-Defined attack patterns, signatures and defense actions for
 - *Layer 7 Access Control List*
 - *Keyword / Phrase Filtering*
 - *URL Filtering*
 - *Application Filtering*
- Real-time alert system, can inform the administrator through Console, E-mail, SNMP
- Auto signature update
- Auto kernel upgrade
- Robust encrypted remote management interface

NK 5100 hardware specification

- Four 10/100/1000 Based-Tx Gigabit Ethernet interfaces (2 x IPS, 1 x HA, 1 x Mirror)
- Two 1000 Base - SX Gigabit fiber interfaces (2 x IPS)
- Support HA architecture
- IPS active at copper or fiber interface
- 9-pin RS-232 serial port (Console)
- Power Supply: AC Line 100-240VAC, 50-60Hz, 250W (MAX)
- Built-in Copper Fail open Hardware Bypass
- Dimension: Standard 19 inches 1U Chassis, 428.6 mm (Width) x 360 mm (Depth) x 44 mm (Height)

BroadWeb Extensible Management System

Hardware Requirements ▶

	Minimum	Recommended
CPU	P4 2.4GHz	P4 2.8GHz or above
Memory	1GB	2GB or above
Hard Drive	40GB	60GB or above
OS	Windows XP Professional	

- Java-based Web GUI
- Centralized Management to control multiple NetKeeper 5100 series appliances simultaneously
- 3-tier remote management architecture
- Real-time attacks and traffic monitoring / analysis in graphic / text mode
- Rule-based policy management
- Role-based access/privilege control
- Links between attack events and policies
- Policies defined by IP and groups
- User defined policies
- User defined report supports SQL command
- Schedule report sent by E-mail or FTP
- Attack event log down to content level
- Auto kernel/signature update
- Supports Syslog
- Export report to CSV and HTML format



- **BroadWeb Corporation:**
857 Hinckley Road, Burlingame, CA 94101 USA
- **Asia-Pacific Headquarters:**
4F, No.8, Hsin-Ann Rd., Hsinchu Science Park, Hsinchu, 300, Taiwan, ROC

