

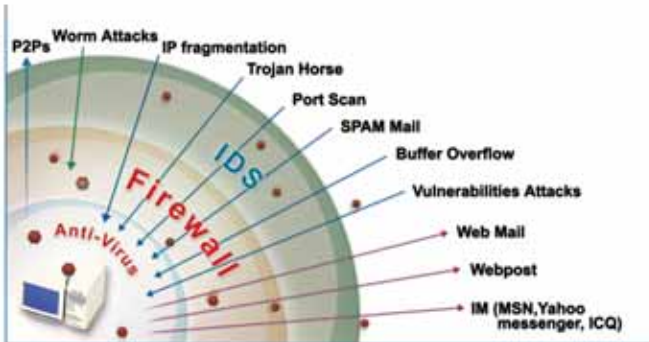
Advanced Intrusion Detection & Prevention

NetKeeper



- Anti - Intrusion
- Anti - DoS / DDos
- Anti - P2P
- Anti - Instant Messenger
- Anti - Worm
- Anti - Porn
- Anti - Web Post

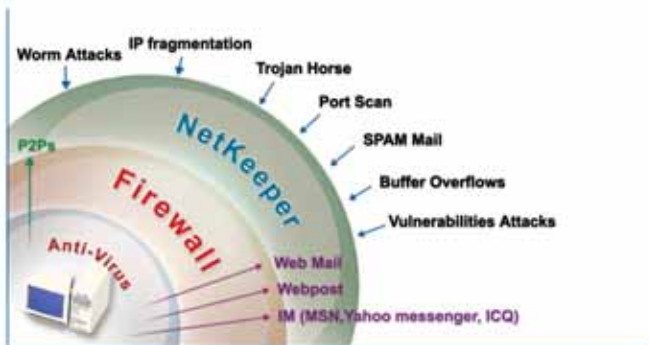
NetKeeper VS. Firewall / Anti-Virus / IDS



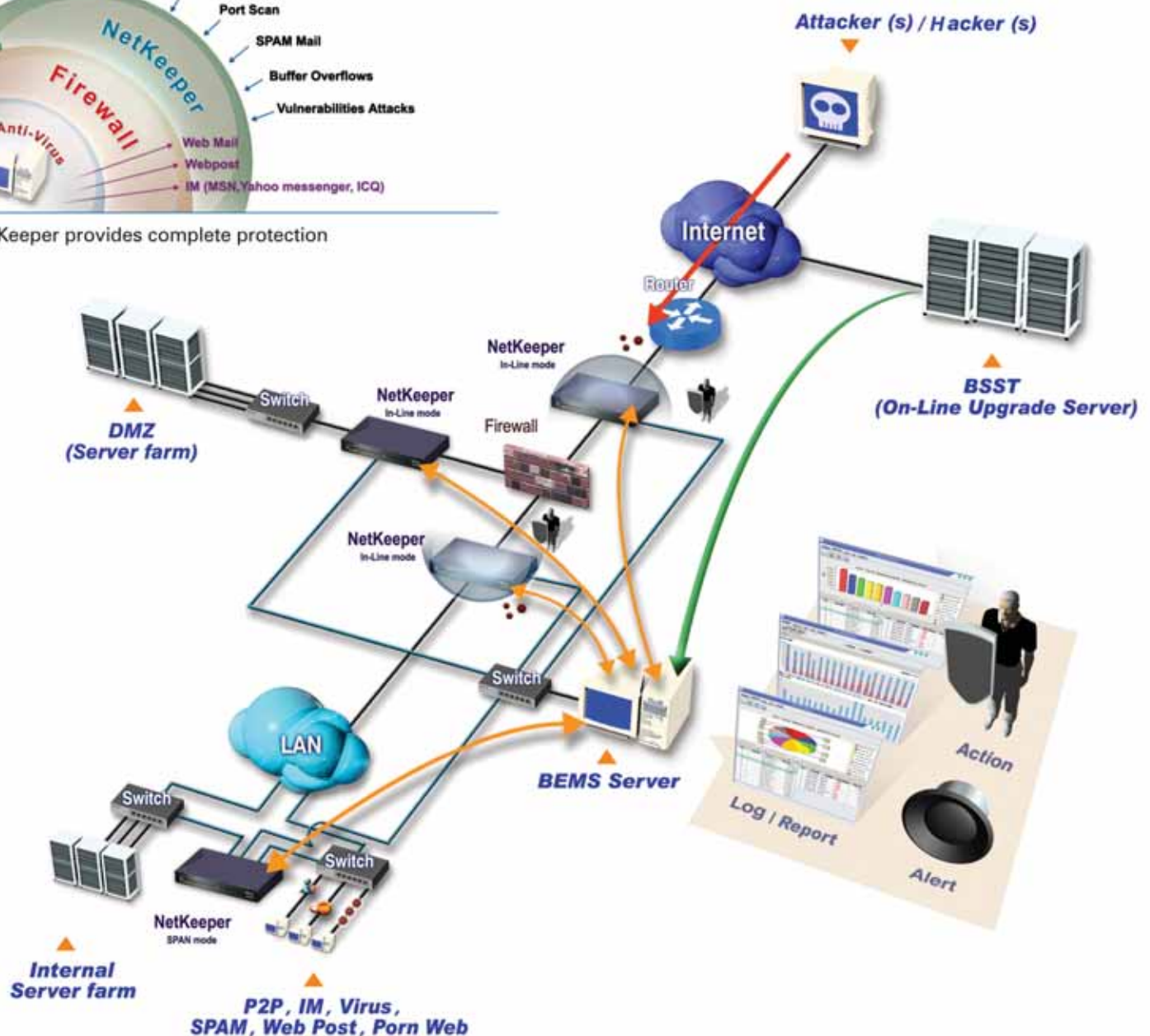
Firewall / anti-virus programs cannot provide protection effectively

NetKeeper can block

- ▶ Buffer Overflow Attack
- ▶ Port Scan
- ▶ Trojan Horse
- ▶ IP Fragmentation
- ▶ Worm Attack
- ▶ System & Application Vulnerabilities Attack
- ▶ DoS / DDoS Attack
- ▶ P2P, IM, Virus, SPAM, Web Post, Porn Web etc.



NetKeeper provides complete protection





NetKeeper
Advanced Intrusion Detection & Prevention

NetKeeper software specification

- Real-time analysis of network traffic to detect malicious codes and attacks
- Supports multiple modes of network operation
 - In-Line
 - Tap
 - SPAN
 - Monitor
 - Bypass
- Contains more than 1700 signatures , including
 - Anti-Intrusion
 - Anti-DoS / DDoS
 - Anti-P2P
 - Anti-Instant Messenger
 - Anti-Worm
 - Anti-SPAM
 - Anti-Porn
 - Anti-Web Post
- Maximum IDP engine throughput:150Mbps
- Highly Secure Embedded Real-Time OS
 - Supports Stealth mode
 - Supports SNMP v2
 - Support Unlimited VLAN tagging
- Multiple-detecting 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
- Configurable software-based bypass function

NetKeeper hardware specification

- Three 10 / 100Based-Tx Ethernet interfaces
- DB9 RS-232 serial port
- Power Supply: AC Line 90-264VAC , 50-60Hz 1A MAX
- Built-in Fail Open Hardware Bypass
- Dimension: Standard 19 inches 1U Chassis , 445 mm (Length) x 265 mm (Width) x 45 mm (Height)

BroadWeb Extensible Management System

Hardware Requirements ▶

| | Minimum | Recommended |
|-------------------|------------|------------------|
| CPU | P4-1.8G | P4-2.4G or above |
| Memory | 512MB | 1GB or above |
| Hard Drive | 20G | 40G or above |
| OS | Windows XP | |

- Java-based Web GUI
- Centralized Management to control multiple NetKeeper 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:
222 S. Harbor Blvd. #680, Anaheim, CA 92805, USA
Asia-Pacific Headquarters:
3F, 24-1, Industry East Rd. IV, Science Based Industrial Park, Hsin-Chu, Taiwan 300 R.O.C.

