

Advanced Intrusion Detection & Prevention

Giga NetKeeper



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

Giga NetKeeper

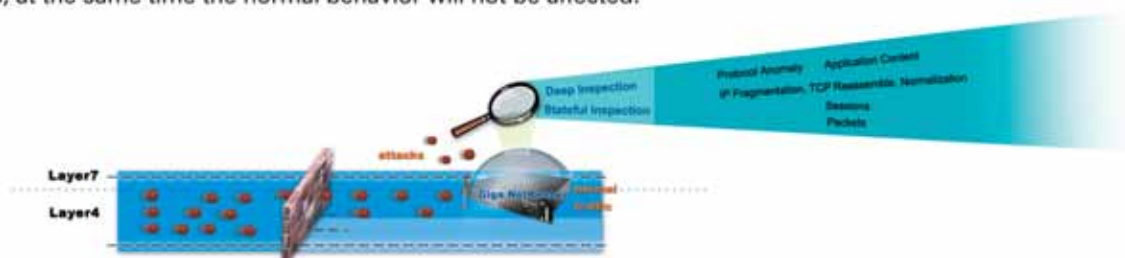
Intrusion Detection and Prevention System

Multiple Functioning Prevention Systems

- ▶ Giga NetKeeper protects the corporate network from being invaded adversely, it also can block Worms, SPAM mail, P2P programs, IM(instant messenger), Webpost and pornographic websites. These functions may well improve the productivity of employees and the effectiveness of bandwidth utilization.

Deep Packet Inspection

- ▶ Since firewalls cannot check the contents of the packets above layer four, many malicious programs can penetrate firewalls with little effort. Firewalls protect the network by blocking the service ports that attack programs use, but this may also block normal protocol propagation. Giga NetKeeper is armed with deep packet inspection, in addition to the verification of the fourth layer of the packets; deep inspection checks into the contents in application layer. Giga NetKeeper can transparently block malicious codes, at the same time the normal behavior will not be affected.



Multi-detection Technique

- ▶ Giga NetKeeper applies an advanced network anomaly behavior analysis technique, anomaly packet analysis technique and multi-string matching technique on attack signatures. Even under the heavy attacks of hackers or worms, Giga NetKeeper is able to ensure multiple layers of security and reduce the false alarm.

Real-time Detection / Destruction at the Boundary

- ▶ Giga NetKeeper accurately detects network intrusion, it can actively block the packets containing malicious codes before they can ever enter your network. This is the solution for real-time Intrusion Detection & Prevention.

Real-time Response to the Attack

- ▶ Giga NetKeeper actively secures Intranet. According to the security policy, it blocks and drops the illegal connection, responds against the attack, and informs the network administrator through all the ways it may find to elaborate effective processes in protection.

Logs and Analyzes All Intrusion Events Completely

- ▶ Giga NetKeeper 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 source, target IP addresses, connection ports and communication protocols.

BEMS (BroadWeb Extensible Management System)

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

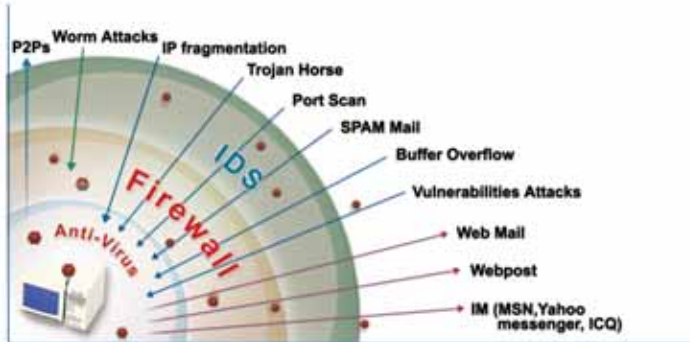
Easy-to-use and Query-on-demand Reporting

- ▶ BEMS also makes it easy to manage tasks of report inquiries, such as top-30 intrusion events, attackers, and victims. All of the daily, monthly and regular reports can be printed and sent out in the CSV 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 Giga NetKeeper. 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 services. BSST will provide technical supports, network security consultation and publish weekly security alerts. They are also responsible for professional training and issue certificate for Broadweb Certified Information Security Professionals (BCISP).

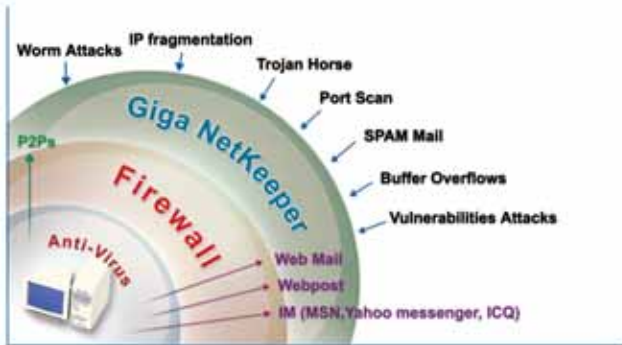
Giga NetKeeper VS. Firewall / Anti-Virus / IDS



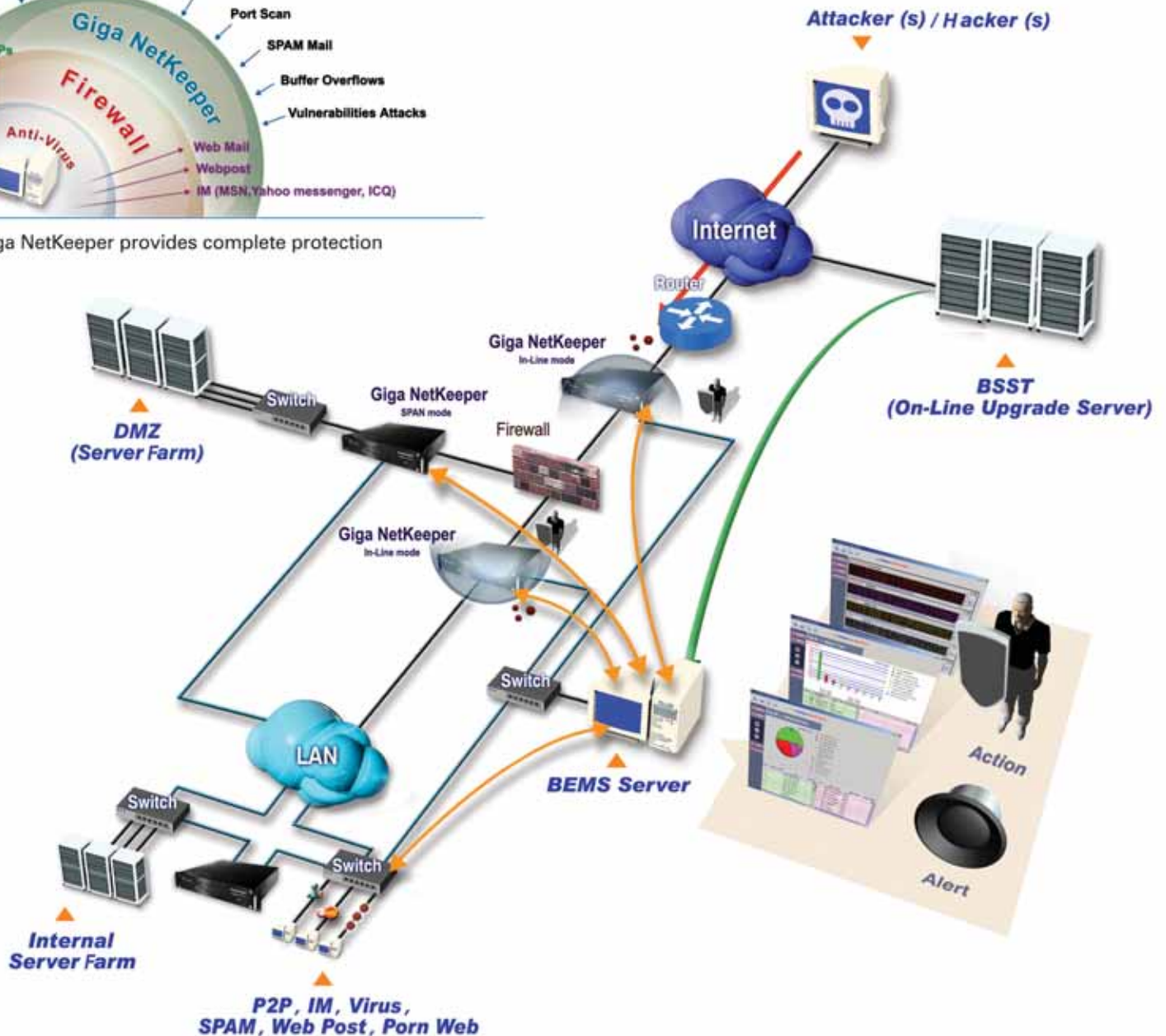
Firewall / anti-virus programs cannot provide protection effectively

Giga 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.



Giga NetKeeper provides complete protection





2004 Best choice of Computex 2004
 2003 Outstanding I.T. Applications / Products Award of IT Month 2003

Giga NetKeeper software specification

- Real-time analysis of network traffic to detect malicious codes and attacks
- Supports multiple modes of network operation
 - In-Line
 - SPAN
 - Bypass
- Contains more than 1,700 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:800Mbps
- 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
 - Keyword/Phrase Filtering
 - URL Filtering
 - Application Filtering
- Real-time alert system, can inform the administrator through E-mail or SNMP
- Auto signature update
- Auto kernel upgrade
- Robust encrypted remote management interface
- Configurable software-based bypass function

Giga NetKeeper hardware specification

- Network Processor-based hardware architecture
- 2 Gigabit Ethernet 1000Base-SX Fiber Optics interfaces
- 4 Fast Ethernet 100Base-TX interfaces
- DB9 RS-232 serial port
- Redundant Power Supply: 110-240V AC, 2-4A, 50-60Hz
- Built-in Fail Open Optical Hardware Bypass
- Dimension: Standard 19 inches 2U chassis, 425.6mm (Length) x 429.6 mm (Width) x 88 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 Giga 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.

