

Advanced Intrusion Detection & Prevention

NetKeeper Eulen



- **ACL-based Firewall Policy**
- **Anti-Intrusion**
- **Anti-DoS / DDoS**
- **Anti-Virus / Worm**
- **Anti-Instant Messenger**
- **Anti-P2P**
- **Anti-Web Mail**
- **Anti-Web Post**

Intrusion Detection and Prevention System ▶



Multi-Functional Network Security Appliance

Not only more hacker activities, new worms and DoS/DDoS will be coming from outside. P2P, Instant Messenger, Trojan, SoftEther and other software popular on Internet also pose threats to your network security from within. NetKeeper Eulen™ utilizes Firewall and IPS (Intrusion Prevention System) functionalities into one box, effectively protects corporate network against Intrusion, Virus, Worm, and SPAM mails. To improve the productivity of employees and the effectiveness of bandwidth utilization, NetKeeper Eulen™ also provides the ability to identify and block applications such as P2P software, Instant Messenger, Web Mail and Web Post. This comprehensive appliance unifies multiple security defense mechanisms on a single protection engine, thus to ensure continuous business and network operation at lowest cost.



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. NetKeeper Eulen™ is armed with Deep Packet Inspection, in addition to the verification of the fourth layer of the packets, Deep Packet Inspection checks the contents in application layer. NetKeeper Eulen™ transparently blocks malicious codes, unwanted traffic and allows legitimate traffic to pass unhindered.

Intrusion Detection and Prevention System ▶



Detailed Log of Security Incidents, Supporting Log Exporting

NetKeeper Eulen™ can fully record the tracks of security incidents. Network administrators can easily trace attack source, destination IP address, connection ports, communication protocols and reactions been taken through the build-in Java-based GUI. Event report can either be sent to designated e-mail address or be exported to pre-assigned server through syslog format.



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 Eulen™. They are committed to study the latest hacking exploits and vulnerability reports over Internet communities. With the knowledge they define the latest defensive policies and provide clients the continuous security service. BSST provides technical supports, network security consultation and publishes weekly security alerts. They are also responsible for professional training and issue certificate for Broadweb Certified Information Security Professionals (BCISP).



Multi-detection Technique & Real-time Response to the Attack

To provide best accuracy, NetKeeper Eulen™'s award-winning detection engine utilizes multiple detection mechanisms, including anomaly behavior analysis technique, anomaly packet analysis technique and multi-string matching technique. According to the security policy configured by the administrator, NetKeeper Eulen™ blocks and drops illegal connection, takes action against the attack, and informs the network administrator through many ways to elaborate effective processes in protection. Even under heavy load of hacker attacks or worms, NetKeeper Eulen™ is able to ensure multiple layers of security and reduce false alarms. to ensure multiple layers of security and reduce false alarms.

NetKeeper Eulen™ Hardware specification ▶



- Three 10/100 Based-Tx Ethernet interfaces
- 9-pin RS 232 parallel port
- Build-in Fail-Open hardware bypass
- LCM display to monitor system and traffic status
- Network utilization panel display (Blue LED)
- Security event panel display (Red LED)
- Power Specification : 5V DC, 4A



BroadWeb

Empower Your Network Security

BroadWeb Corporation:

222 S. Harbor Blvd. #680, Anaheim, CA 92805, USA

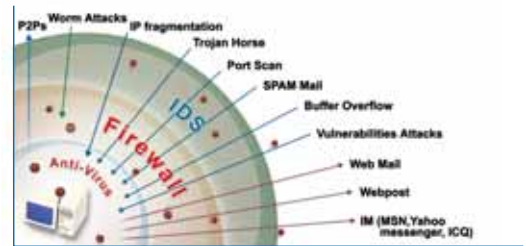
Asia-Pacific Headquarters:

3F, 24-1, Industry East Rd. IV, Science Based Industrial Park, Hsin-Chu, Taiwan 300 R.O.C.



NetKeeper Eulen™ Specification ▶

- Concurrent connections:10,000
- IPS performance:35Mbps
- Support multiple modes of network operation
 - In-Line Mode
 - Monitor Mode
 - Bypass Mode
- ACL-based firewall policy
 - Layer 4 Access Control (TCP / UDP / ICMP / IGMP)
 - Bi-directional (LAN to WAN ; WAN to LAN) user-definable
- Intrusion Detection and Prevention System
 - Contains more than 1,700 signatures ,including
 - Anti-Intrusion
 - Anti-DoS / DDoS
 - Anti-P2P
 - Anti-Instant Messenger
 - Anti-Virus / Worm
 - Anti-SPAM
 - Anti-Web Mail
 - Anti-Web Post
- Multiple-detection engine that combines Misuse and Anomaly Detection technologies.
- Actively filter and drop malicious TCP/UDP/ICMP/IGMP packets, and can reset the TCP connections.
- Highly Secure Embedded Real-Time OS
- Configurable threshold parameters to fit into different network environment.
- User-Defined attack patterns, signatures and defense actions.
- Support Stealth Mode.
- Support SNMP.
- Support Unlimited VLAN tagging.
- Build-in Java-based Graphical User Interface.
 - Monitoring real-time packet flow status, connection numbers, and detailed security events.
 - Log in detail of the source and target IP addresses, connection ports, communication protocols, packet contents and event time period.
 - Real-time alert by E-mail and Syslog.
- Automatically on-line signatures upgrade.
- Automatically on-line kernel upgrade.
- Configurable software-based bypass function.



Firewall / anti-virus programs cannot provide protection effectively



NetKeeper Eulen™ provides complete protection



ISO 9001 : 2000

