

## Advanced Intrusion Detection & Prevention

# NetKeeper 6000



### Multi-Functional Network Security Appliance

- ▶ Not only do hacker activities occur in high frequency nowadays, but also the fact that more worms/viruses and DoS/DDoS can penetrate into the private networking systems from outer world with minimal effort. P2P, Instant Messenger, Trojan, SoftEther, together with many other popular spy software found on the Internet also pose tremendous threats to your network security internally and externally. NetKeeper 6000 integrates Firewall and IPS (Intrusion Prevention System) functionalities into one box, effectively protecting corporate network against Intrusion, Virus, and Worm. Besides, users are able to control the quota of network bandwidth and limit bandwidth usage of specific target or signature, which can significantly increase network bandwidth and network application efficiency.

### Flexible Deployment and Virtual IPS

- ▶ NetKeeper 6000 furnishes unprecedented flexibility of deployment, including IPS, IPS monitor, IDS, IDS monitor and HA. It suits to any type of network security architecture and the user is able to configure different type of protection on each interface. Moreover, NetKeeper 6000's comprehensive Virtual IPS setting allows the capability to segment an IPS port pair into a large number of virtual IPSes, each with its own security policy. Each pair of IPS port has its own virtual IPS rule-set as well. The flexible deployment and virtual IPS setting fit the NetKeeper 6000 to any network architecture and provide highly customized and granular security policies for a dramatic reduction in false-positives.

### Vulnerability-Based Virtual Patch Protection

- ▶ NetKeeper 6000 incorporates "virtual patch" protection to new vulnerabilities even before exploits are developed. Basically there is a "blind spot" of about a few weeks between the announcement of a typical vulnerability and an exploit against it. Most enterprises take extended time to patch their PCs and servers. BroadWeb virtual patches are developed as soon as the vulnerabilities are discovered, and continuously applied to the NetKeeper 6000 to make sure it is up-to-date against the latest vulnerabilities so that the purpose of proactive protection against unpatched systems is achieved. This innovation of vulnerability-based virtual patch doesn't focus on exploits, but rather on the vulnerability that precedes the attack.

### BEMS (Broadweb Extensible Management System)

- ▶ BEMS (Broadweb Extensible Management System) is a Java-based central management program that is designed to manage multiple NetKeeper 6000 appliances at the same time. Integrating with Plug-ins, BEMS provides a user-friendly interface to monitor the real-time network traffics, real-time security-events, and allows users to modify policies and even defines their own policies.

### 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 6000.

#### STATEFUL TRAFFIC INSPECTION ▶

- IP Defragment and TCP Reassembly
- Protocol Normalization
- Protocol Analysis
- Protocol Enforcement
- Evasion Prevention
- Protocol Tunneling

#### EMAIL PROTECTION ▶

- Anti-Virus\*
- \* Future firmware / hardware upgrade

#### ANOMALY DETECTION ▶

- DoS / DDoS
- Port Scanning
- Application Anomaly
- Spoof Detection
- IP Sweeping

#### FIREWALL ACL ▶

- TCP / UDP / ICMP SPF
- Per Rule Rate Limit
- Per Rule Quota Control

#### SIGNATURE DETECTION ▶

- User-defined Signature
- Real-time Signature Update
- Virtual IPS
- Per Rule and VIPS Rate Limit
- Per Rule and VIPS Quota Control

#### HIGH AVAILABILITY ▶

- Hardware Bypass

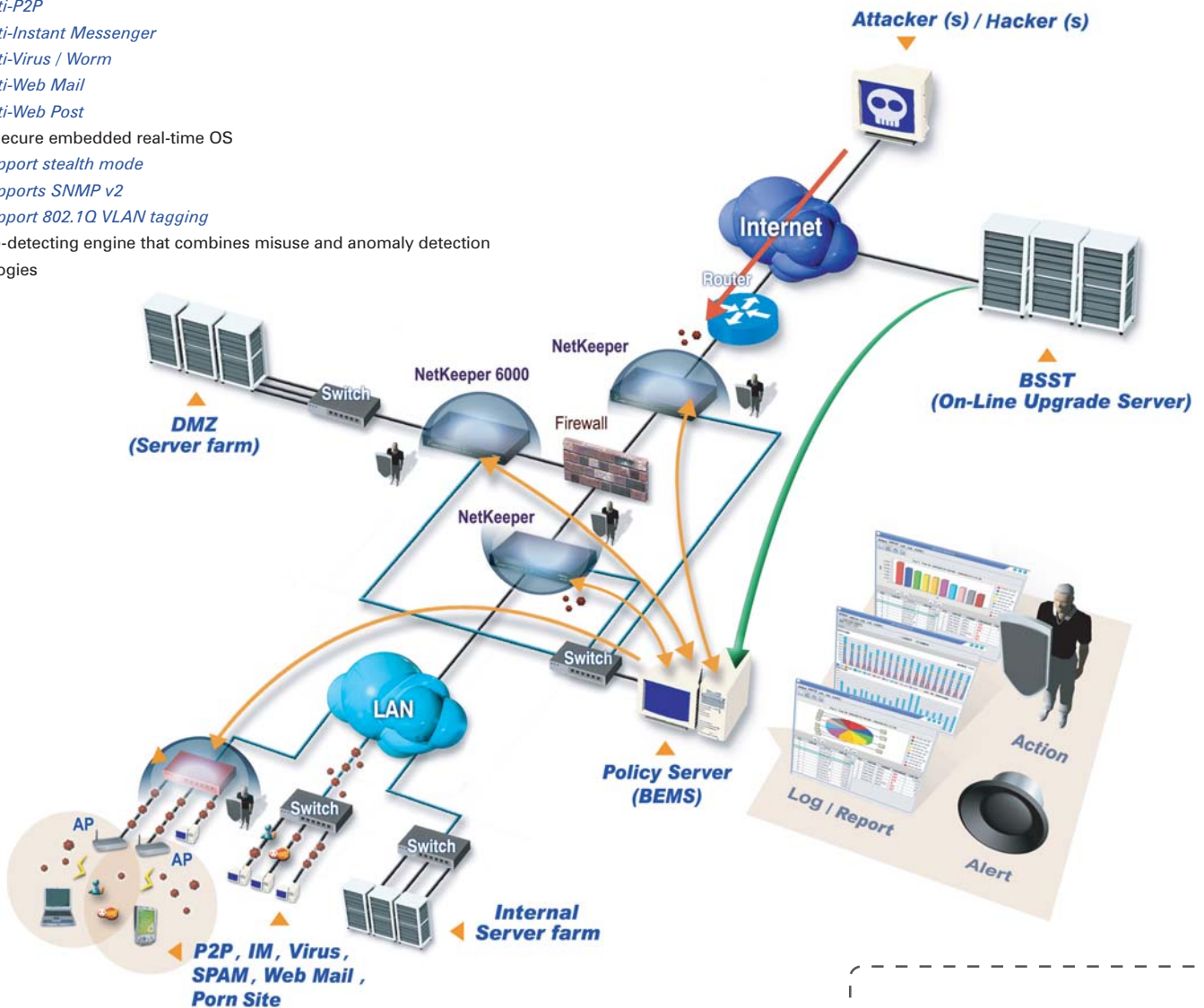
## NetKeeper 6000 Hardware Specification

- Seven (7) 10/100/1000 Mbps copper
- DB9 RS-232 Serial Port
- Built-in selectable hardware bypass
- Dimension: Standard 19 inches 1U Chassis  
429mm (Width) x 360mm (Depth) x 44mm (Height)
- Power Supply: AC Line 100-240VAC, 60~50Hz, 6~3A

## NetKeeper 6000 Software Specification

- Real-time analysis of network traffic to detect malicious codes and attacks
- Supports multiple modes of networks operation
  - IPS
  - IPS Monitor
  - IDS
  - IDS Monitor
  - Forward
- Contains more than 1700 signatures, including
  - Anti-Intrusion
  - Anti-DoS / DDoS
  - Anti-P2P
  - Anti-Instant Messenger
  - Anti-Virus / Worm
  - Anti-Web Mail
  - Anti-Web Post
- Highly secure embedded real-time OS
  - Support stealth mode
  - Supports SNMP v2
  - Support 802.1Q VLAN tagging
- Multiple-detecting engine that combines misuse and anomaly detection technologies

- Detect anomaly behaviors using multiple detection methods, including protocol and traffic anomaly analysis
- Actively detect and block packets 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 4 / 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
- Support per rule rate limit to specific target or signature
- Support per rule quota control to specific target or signature
- Support high availability
- Support virtual IPS / IDS , it can be defined according to IP addresses, port(s), interfaces and VLAN ID
- A Virtual IPS has individual layer 4 ACL (Access Control List)
- Build-in Virus-detection engine and Virus definition database



 **BroadWeb**  
Empower Your Network Security

- **BroadWeb Corporation:**  
857 Hinckley Road, Burlingame, CA 94010 USA
- **Asia-Pacific Headquarters:**  
4F, No.8, Hsin-Ann Rd., Hsinchu Science Park,  
Hsinchu, 300, Taiwan, ROC



[http:// www.broadweb.com](http://www.broadweb.com) E-mail: [partner@broadweb.com](mailto:partner@broadweb.com)