



**BroadWeb**

Empower Your Network Security



***A White Paper By BroadWeb  
Corporation***

**<http://www.broadweb.com>**



## FORWARD

The convenience of the Internet has created a tremendous worldwide venue for commerce and information sharing. Unfortunately, this same convenience creates tremendous network security problems. In the past, the industry used firewalls as the main tool to ward off intrusions by hackers. But as network attack patterns become more varied and complicated, a simple firewall fails to meet the security requirements of the modern commercial environment. Intrusion Detection Systems (IDS) are the most recent innovation in the invasion detection arms race. In addition to inspecting all inbound and outbound packets, IDSs block the prototypical Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks.

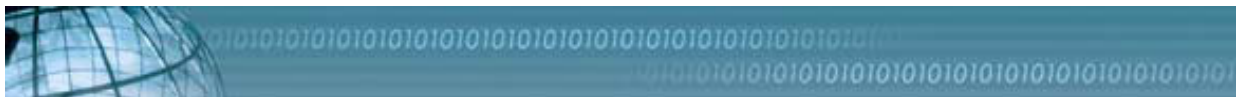
An added challenge in the recent years has been so-called Network Worms, which do an exemplary job at escaping anti-virus software. A recent example of the devastation these can wreak was provided by the SQL Slammer in 2003, which within 10 minutes of the attack, 67,000 servers were infected. 5 hours later, 120,000 servers had been compromised all around the world. This type of worms does not create or modify any files but remains hidden from traditional anti-virus software inside memory. Only IDS can effectively resist attacks from this type of network worms.

The 2003 Network Attack Trends Analysis of Computer Emergency Response Team (CERT® /CC)\* has identified the following 6 trends in the world of network attacks ([http://www.cert.org/archive/pdf/attack\\_trends.pdf](http://www.cert.org/archive/pdf/attack_trends.pdf)):

1. Automation; speed of attack tools
2. Increasing sophistication of attack tools
3. Faster discovery of vulnerabilities
4. Increasing permeability of firewalls
5. Increasingly asymmetric threat
6. Increasing threat; infrastructure attacks



NetKeeper™ AIDP is a Network Intrusion Detection and Prevention System (NIDP). It is able to detect intrusions and take the appropriate actions to prevent the users' network or server host from the harm. NetKeeper™ AIDP is especially effective when blocking Denial of Service (DoS)/Distributed Denial of Service (DDoS) attacks, Virus/Worms and other unwanted network applications such as Peer-to-Peer or Instant Messenger program. In the following chapters, we will discuss the related idea of the Intrusion Detection and Prevention System, the concept and technologies of the DoS and DDoS attacks, and how NetKeeper™ AIDP works to prevent those attacks.



## Chapter 2 Preventing DDoS Attacks with NetKeeper™ AIDP

Standard firewalls and IDS would attempt to identify a DDoS by simply analyzing the amount of incoming data. When the number of data exceeds the normal rate, the firewall or IDS will issue alert. Unfortunately, this method is much too simple to provide real protection against DDoS attacks.

NetKeeper™ AIDP handles DDoS attacks with a more complex strategy. First, NetKeeper™ AIDP checks if there are any control packets from the attackers to the client sites or from the client sites to the Daemons. If there are, NetKeeper™ AIDP will block their communication and spoil the attacks. At the same time, the system inspects the attack reports for new Trojan Horses and foreign Daemons scripts. Figure 1 shows the default defense policies for a DDoS attacks.

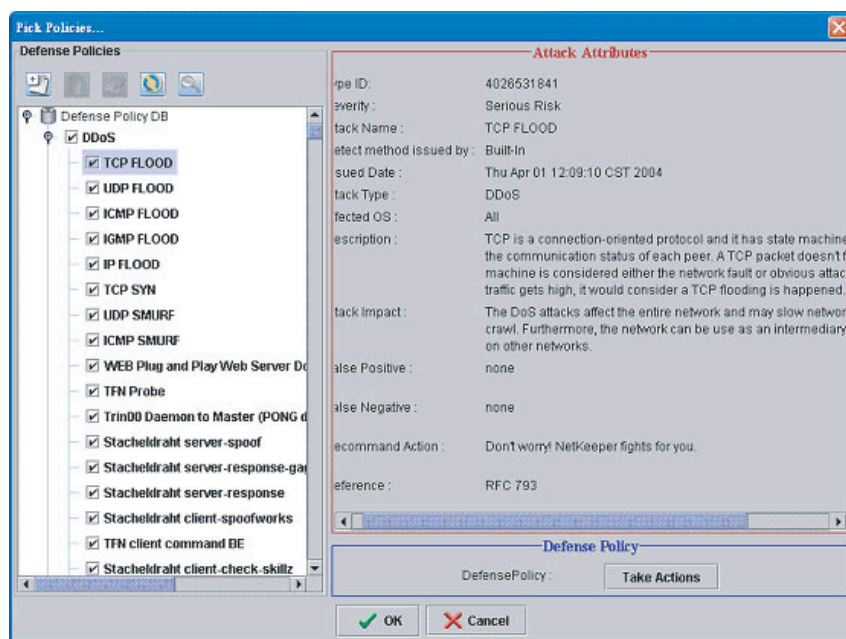
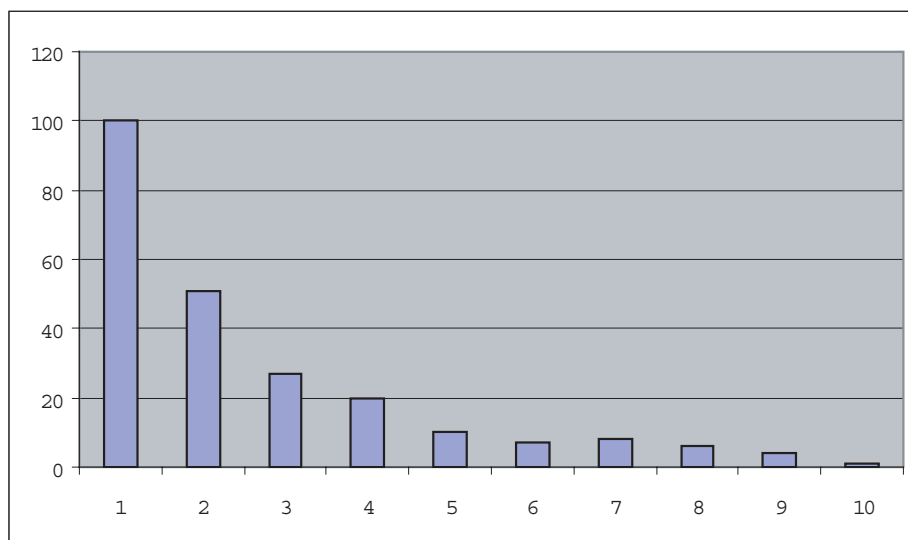


Figure 1: Default Defense Policies for DDoS Attacks with NetKeeper™ AIDP



NetKeeper™ AIDP also features a detection module to search for common network anomalies such as SYN Flooding, TCP Flooding, ICMP Flooding, UDP Flooding, IGMP Flooding, UDP Smurfing, ICMP Smurfing, Port Scan, and Bad IP packets.

Once a second, NetKeeper™ AIDP normalizes, transforms and compares the data to baseline. An alert is issued when the result of the comparison is abnormally high. The advantage of this is a decreased risk of misinterpretation due to the packets size. The selected baseline is an academic research standard, but NetKeeper™ AIDP allows the users to adjust the settings for their network environment. Figure 4 illustrates this setup screen.



*Figure 2: The Network Packet Distribution Chart of the Baseline*

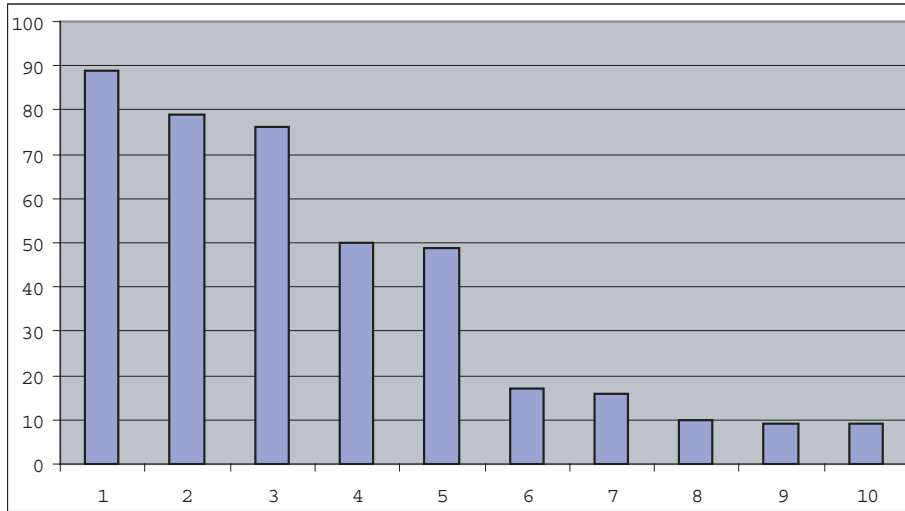


Figure 3: The Network Packet Distribution Chart of the Possible Anomalies

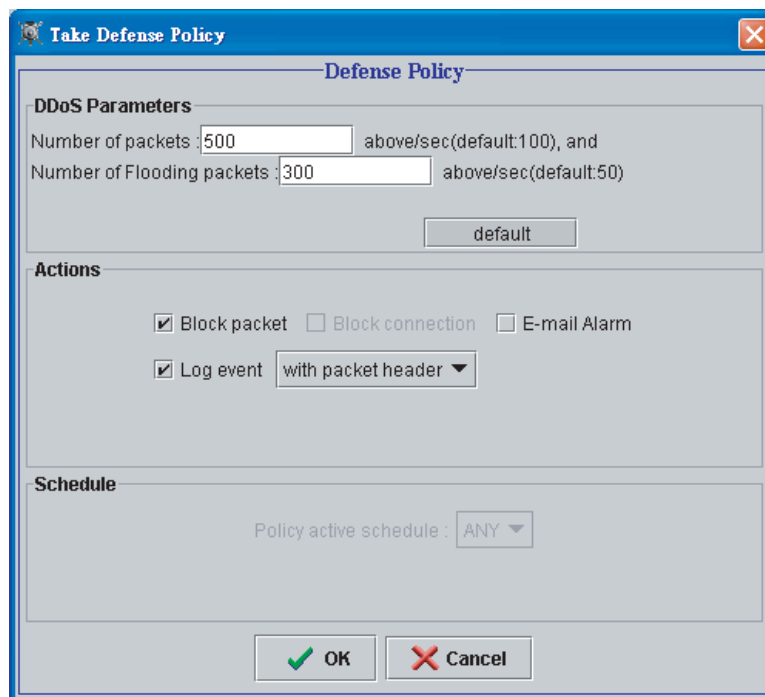


Figure 4: The Parameter Settings for DDoS Detection



## Chapter 3    The Detection Technology of the Network Intrusion Detection and Prevention System (NIDP)

Whether or not NIDP is able to effectively detect the hackers' attack packets depends on the applied technology, recognizing a sufficient collection of the attack patterns.

Generally speaking, the technologies NIDP employs can be divided into 2 categories: Anomaly Detection, and Misuse Detection. There are several methods of detecting network anomalies. The most frequent used method is statistical analysis. This method detects attacks by comparing the statistical parameters of the observed network traffic with normal traffic, and it is not necessary to collect the hackers' attack patterns. This is especially effectively when detecting new attack patterns. Yet, the weakness of this method is the possibility of misinterpretation. Parameter settings need to be provided for the users to adjust threshold to best fit their network environment. This method is mostly used to detect Distributed Denial of Services (DDoS) attacks.

In addition to the standard statistic Anomaly Detection, NetKeeper™ AIDP also uses Protocol Anomaly Detection, Port Scan Detection, and Fragmented Packet Reassemble Detection to effectively reduce the possibility of the misinterpretation incurred by the typical anomaly detection.

Another technology commonly used by the NIDP is Misuse Detection. This detection compares the attack packets' signatures with the ones in the NIDP signature database. Therefore NetKeeper™ AIDP is able to detect and block Code Red, Code Blue, and Code Rainbow viruses before the viruses penetrate into victim's network. This is more effective than the traditional means of anti-virus software detection, which doesn't occur until the viruses arrive at the server. An advantage of this technology is the accuracy of detecting known hackers' signatures by matching analysis. The disadvantage is that the NIDP is unable to detect and prevent new attack patterns before patterns are reported and signatures are made. Consequently, an effective signature match system needs frequent database updates.

NetKeeper™ AIDP's signature match detection technology employs several different detection methods to augment the accuracy and efficiency of detection. They include:

- *Signature Database*



- Multiple Pattern Matching
- Backdoor Detection
- Trojan Horse Detection
- User-defined Detection

The network defense policy is the most significant feature in NetKeeper™ AIDP's Management System. Because of the network defense policy, NetKeeper™ AIDP knows when to detect attacks, what actions to take, what to protect and when to protect it. Figure 5 is the screen capture of the actual NetKeeper™ AIDP's defense policy window.

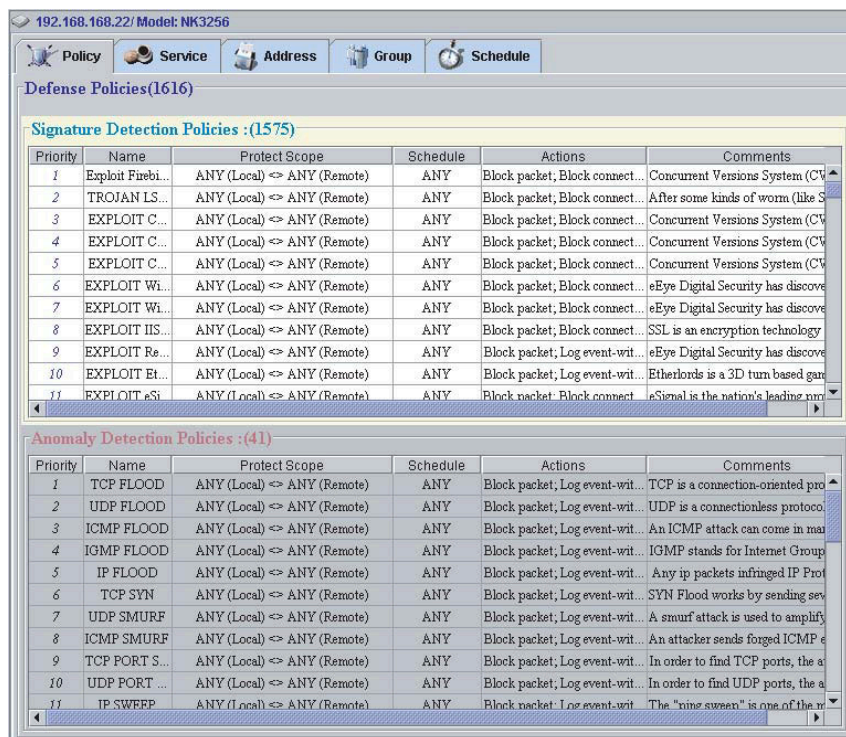


Figure 5: NetKeeper™ AIDP defense policy window

There are more than 1,600 defense policies in NetKeeper? AIDP. The users can select the defense policies that are the best for their network environment, the operating system of their server and employed software applications. These defense



policies include actions to protect various operating systems (i.e. Windows 95/98, Windows NT, Windows 2000/XP, Linux, FreeBSD, Solaris, SGI, and etc.), network equipments, and application programs (i.e. bind, sendmail, Exchange, pop3d, imapd, ws\_ftp, Peer-to-Peer, Instant Messenger and etc.). Moreover, NetKeeper™ AIDP allows for heavy defense policy customization, shown in Figure 6. The users should understand hackers' attack pattern to customize their own defense policies. However, NetKeeper™ AIDP employs a team of experts called BSST who constantly collect hackers' attack patterns and create new defense policies to ensure the network is safe from the latest attacks.

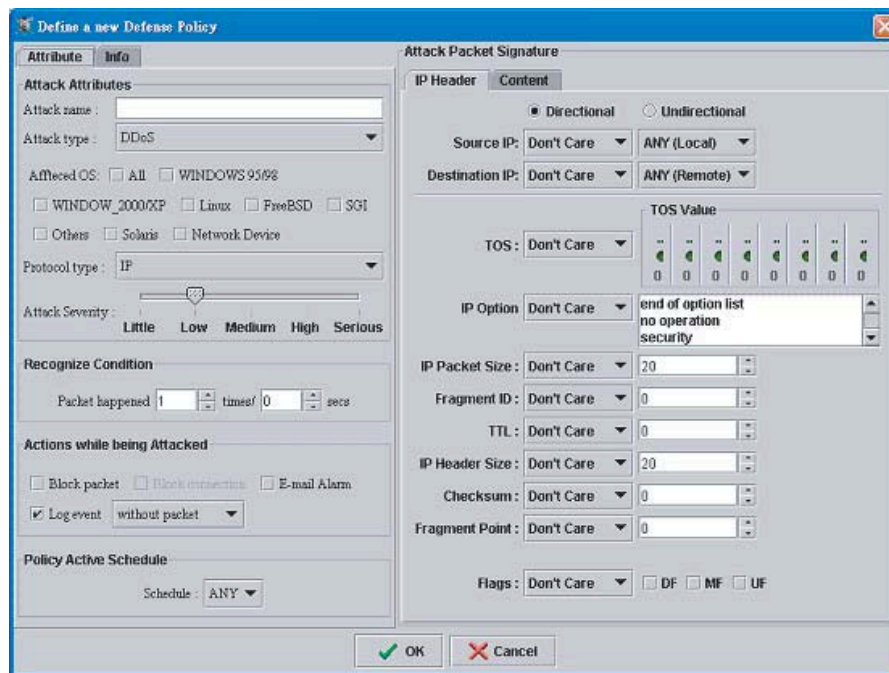


Figure 6: Defense Policy Customization



## Chapter 4 Requirements for the Network-based Intrusion Detection and Prevention System

This chapter describes the requirements of network-based intrusion detection systems (NIDP).

### 1. Passive NIDS And Active NIDP

Passive NIDS works with the Port Mirroring function of the Switch or Hub and passively monitors all passing packets. After analyzing and comparing the packets with its attack data, Passive NIDS discriminates normal network traffic from malicious attack packets. If an anomaly is found, Passive NIDS will alert through its management interface or inform the firewall to block the connection. By this time, however, it might be too late.

Active NIDP has all the abilities of Passive NIDS. Moreover, Active NIDP takes appropriate actions on time to protect the server host and network from damage. It works like a firewall but where the firewall focuses on controlling network resources and only inspects the packet up to Layer 4 protocol. Active NIDP adopts deeper intrusion detection technologies and analytical ability to Layer 7 protocol. Active NIDP is a transparent network system and operates as In-Line mode. It receives the packets from one end of the network, examines them through the intrusion detection engine, and then filters them. Consequently, Active NIDP does not allow the damage caused by timing issue.

Typically, Active NIDP is much more accurate and effective than Passive NIDS. Figure 10 illustrates the network structure of Passive NIDS and Active NIDP. Passive NIDS usually needs to work with a specific firewall, whereas Active NIDP is compatible with any firewall. Active NIDS can work independently.

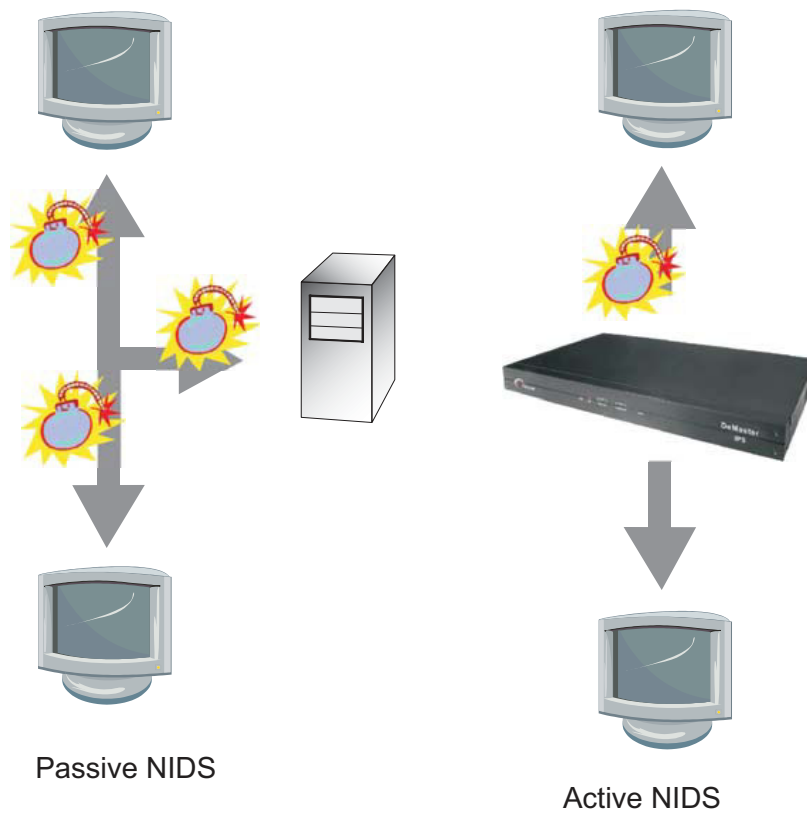


Figure 7: Compares between NIDS and NIDP



## Chapter 5 Overview of NetKeeper™ AIDP

NetKeeper™ AIDP is an in-line Active Network-based Intrusion Detection and Prevention System (NIDP). Without adjusting the network structure, NetKeeper™ AIDP can inspect network packets in real-time, and block possible intrusions.

When NetKeeper™ AIDP detects an attack, it actively filters out the offending packets, blocks connections, activates the defense system, and compiles alerts and logs. NetKeeper™ AIDP combines Misuse Detection and Anomaly Detection technologies to detect and analyze the packets from the Internet or intranet. Because of the combination, NetKeeper™ AIDP is able to protect the network from the existing attacks and detect novel attacks based on flexible defense rules. Moreover, NetKeeper™ AIDP is built with high performance hardware design platform and proprietary real-time operating system, adding a real level of difficulty to hackers' attempts.

### 1. Features

#### ■ *Multiple Functioning Prevention Systems*

NetKeeper can protect the corporate network from being invaded adversely, it can also block Viruses, SPAM mail, P2P on-line download programs, IM instant messenger programs, Webpost and pornographic websites. These functions may well improve the efficiency of employees and the effectiveness of bandwidth use, so the profit of the corporation is increased.

#### ■ *Deep Packet Inspection*

Since firewalls cannot check the contents of the packets above layer four, many attacking programs can penetrate firewalls with little effort. Firewalls protect the network by blocking the service ports that attack program use, but this may also invalidate normal protocol propagation. NetKeeper is armed with deep packet inspection, in addition to the verification of the fourth layer of the packets; deep inspection into the contents in the seventh layer of the packets make it possible to block the penetration of malicious codes. At the same time, the propagation of the normal protocol is not affected.



#### ■ *Multi-detection Technique*

NetKeeper applies an advanced network anomaly behavior analysis technique, anomaly packet analysis technique and multi-detection technique on characteristic attacking codes. Even under the attack of hackers or worms, NetKeeper is able to provide multiple layers of security and protection for the corporation.

#### ■ *Real-time Detection/ Protection at the Boundary*

NetKeeper provides not only precision to detect an invasion, but also blocks the attacking packets or the malicious programs before they enter the intranet. This is the solution to the problems of intrusion prevention.

#### ■ *Real-time Response to the Attack*

NetKeeper actively secures the safety of the intranet. According to the policy setting, 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*

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



■ *Clear and Easy-to-use Reporting System*

NetKeeper's Web-based click-and-select User Interfaces make it easy to manage tasks and report inquiries, such as top-ten intrusion events, attackers, and victims. All of the daily, monthly, and regular reports can be printed and sent out in the HTML format.

■ *Professional BSST (Broadweb Security Service Team)*

BSST (Broadweb Security Service Team) teams up a group of network security experts with a Broadweb security service team. They are committed to studying the invasive methods used by hackers, to collect network security information, to get hold of the signs of weak spots in time, and to provide clients with the service of a safenetwork environment swiftly and continuously. They also define updated defensive policies, provide technique supports, give consultation on security techniques, educate and train users, distribute security alerts and issue certificate for Broadweb Certified Internet Security Professional (BCISP) to qualified engineers.

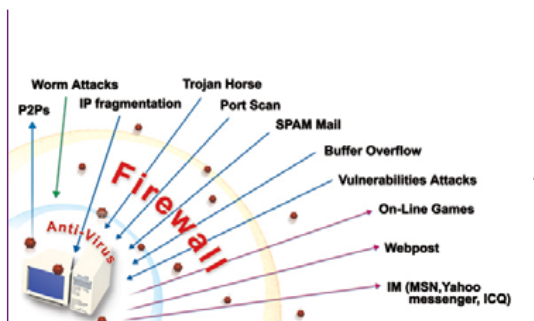
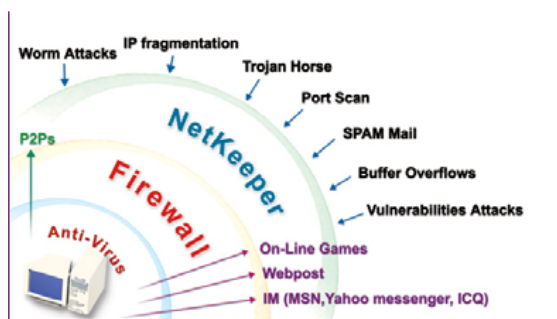


Figure 8: NetKeeper vs Firewall/Anti-Virus

Figure 9: NetKeeper Provides complete protection





## Deployment

NetKeeper™ AIDP is a network transparent device with three-tiers of management structure: multiple NetKeeper™ AIDP appliances, central controlled by Policy Server, a Java-based management server. There is no need to modify users' network structure to install it. The NetKeeper™ AIDP provides multiple operation modes to fit different network deployment including In-Line mode, Tape mode, Span mode and By-pass mode. The deployment of NetKeeper™ AIDP is shown as Figure 9.

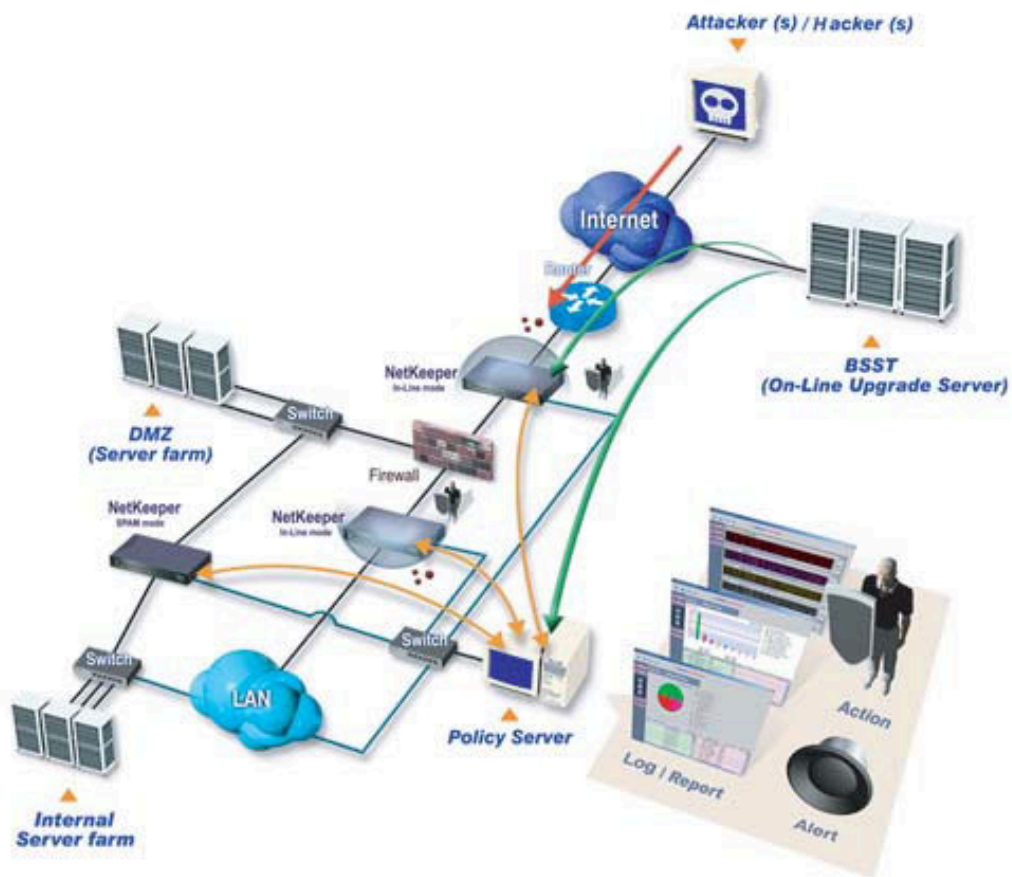


Figure 9: NetKeeper™ AIDP Network Deployment



## Chapter 6 Conclusion

With the Internet's ever-increasing role in the world of commerce and information, systems security is more important than ever. Firewalls have long provided a first line of defense, but secure network today calls for more sophisticated protection, which all network security providers devote to. NetKeeper™ AIDP, a Network-based Intrusion Detection and Prevention System presented by BroadWeb, offers a proven intrusion detection and prevention system with the most efficient performance available today. The enterprises now can focus on their business and have no need to worry about network security.