

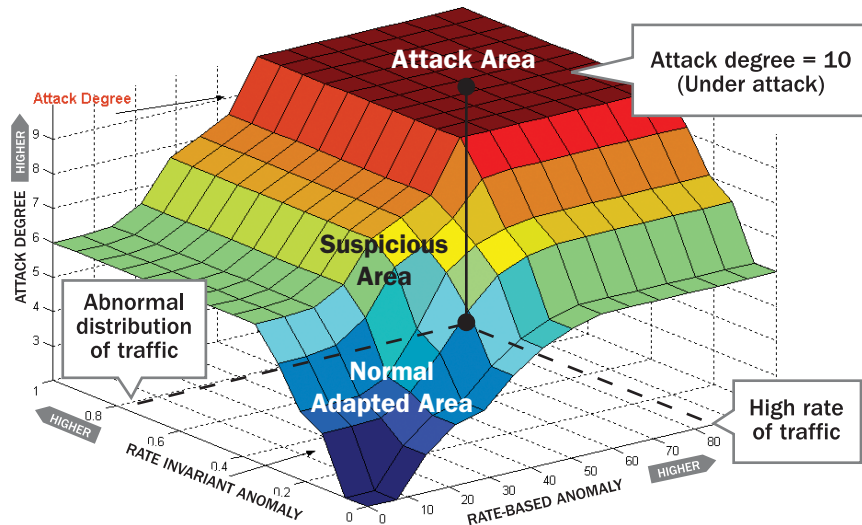
## Block DoS/DDoS Attacks in Seconds While Ensuring High Application Performance



For high-volume, online businesses besieged by Denial of Service (DoS) and distributed DoS (DDoS) attacks, Radware offers a compelling solution: Radware DefensePro-6000. Employing the industry's most advanced, behavior-based technology, DefensePro-6000 provides unmatched protection against both known and unknown DoS/DDoS attacks including HTTP Page flood attacks, while ensuring fast application response times for legitimate users. DefensePro® is ideal for securing high-traffic environments such as online stores, banking, gaming, auction sites, ISPs, DNS sites and registrars.

### Key Business Values

- Ensures Business continuity under network attacks
  - Removes high volume DoS/DDoS floods attacks including HTTP Page Floods
  - Blocks attacks without blocking legitimate users' traffic.
- Reduces total cost of ownership (TCO) of security management.
  - Adapts to changing network conditions
  - Requires minimal configuration without the overhead of system tuning and ongoing maintenance
- Reduces link capacity costs for carriers
  - Removes high volume worm DoS/DDoS flood attacks
  - Fast response to known and zero-day attacks without blocking legitimate users' traffic during attack



**Figure 1: Adaptive Decision Engine**

DefensePro is unique in its ability to rapidly and accurately distinguish between three broad categories of behavior: legitimate normal traffic, attack traffic and unusual patterns created by legitimate activity

DefensePro-6000 integrates multiple protection modules into a single appliance to deliver increased security, faster response times for legitimate applications when under attack, and a lower total cost of ownership (TCO). DefensePro strengths include:

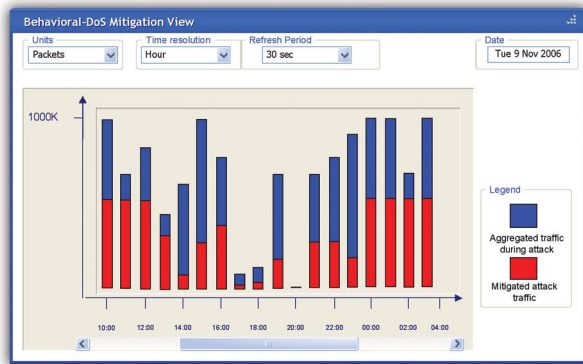
- Multi-gig DoS & DDoS flood protections.
- Adaptive behavior-based technology for known and zero-day DoS & DDoS attacks.
- The fastest response to DoS & DDoS attacks with only seconds required to prevent the most “complex” DDoS flood attack.
- Integrated bandwidth management prioritizes critical applications to ensure the most efficient business continuity.
- High port density, up to 9 segments and two XGE ports allows core network deployments.
- Carrier-grade platform offers dual power supply and internal bypass to maximize uptime and fault tolerance.

#### Highly accurate DoS/DDoS protection

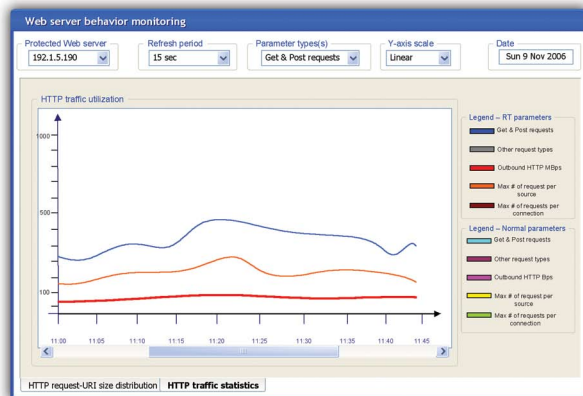
The DefensePro-6000’s behavior-based DoS protection uses adaptive, self-learning and self-adjusting technology to immediately block known and unknown, zero-day flood attacks in seconds (see figure 1)

#### The only HTTP page flood protection solution

The HTTP Mitigator feature deploys the behavioral security technology to prevent HTTP page flood attacks that are often generated by malicious tools such as HTTP BOTs and HTTP page flooders. These tools are used directly by hackers or are installed unwittingly on victim computers. They systematically download web pages from a web site attempting to exhaust its resources and create service denial.



**Figure 2: Real-Time Traffic Monitoring and Mitigation View**  
Real-Time traffic monitoring views expose DefensePro attack mitigation capabilities to the managerial level showing normal traffic vs. attack traffic that was filtered out to provide immediate ROI visualization



**Figure 3: Real-Time Web server behavior Monitoring**  
Real-Time Web servers' traffic monitoring enables the admin to view normal vs. real-time HTTP request distribution rates

### Assured performance, even when under attack

Integrated bandwidth management and access control offers added assurance of business continuity and high application performance by prioritizing bandwidth. Trusted sources are allowed to pass quickly, with improved user response time, while malicious hosts are blocked.

### Enhanced visibility and decision support

Real-time Dashboard and attack monitoring provide administrators with immediate insight into attacks, including top sources and destinations, blocked attacks, and vulnerable resources. Real-time traffic monitoring allows the Admin to observe the normal traffic behavior, web traffic behavior and attacks volume that were mitigated by DefensePro (see figures 2 and 3).

## Radware APSolute™ Product Suite

Radware, the global leader in integrated application delivery solutions, assures the complete availability, performance and security of business-critical applications for more than 5,000 enterprises and carriers worldwide. With Radware's comprehensive APSolute suite of application front end, access, and security products, companies can drive business productivity, improve profitability, and reduce IT operating and infrastructure costs by making their networks "business-smart."

### Certainty Support

Radware offers technical support for all of its products through the Certainty Support Program. Each level of the Certainty Support Program consists of four elements - phone support, software updates, hardware maintenance, and on-site support. Radware also has dedicated engineering staff that can assist customers on a professional services basis for advanced project deployments.

### Learn More

To learn more about how Radware's integrated application delivery solutions can enable you to get the most of your business and IT investments, email us at [info@radware.com](mailto:info@radware.com) or go to [www.radware.com](http://www.radware.com).

## Technical Specifications

<b>DefensePro Model</b>	DefensePro 6000
ASIC-based Hardware Platform	Application Switch 5
<b>Performance<sup>1</sup></b>	
Max. Throughput	6 Gbps
Maximum Concurrent Sessions	Unlimited <sup>2</sup>
Latency (micro-seconds)	< 200
<b>Ports</b>	
XGE (10GE)	2
GE (GBIC)	9
10/100/1000 Copper	8
Console RS-232C	1
<b>Scanning Ports</b>	
Maximum Segments	9
Network Operation	Transparent L2 Forwarding
Deployment Operation Modes	In-line, SPAN port Monitoring and Copy Port
Operation Modes	Block & report, report only
<b>Management Ports</b>	Includes GE, FE and RS-232
<b>Tunneling Protocols Support</b>	L2TP, MPLS, GRE, GTP, VLAN Tagging
<b>Network DoS/DDoS Protections</b>	Adaptive Behavior-based, Zero Day Flood attacks protection for SYN, TCP, UDP, UDP (with ICMP Back Scattering), DNS Query, ICMP, IGMP, IP Fragment Floods. Blocking is done through "Adaptive Smart Dynamic Filters".
<b>HTTP Floods Protection</b>	Adaptive behavior based web server traffic monitoring detecting and preventing known and zero-day HTTP Page Flood attacks. Blocking is done through "Adaptive Smart Dynamic Filters".
<b>Adaptive Smart Dynamic Filters (Packet Filter Criteria)</b>	Source IP, Destination IP, Source Port, Destination Port, Packet ID, Packet size, TTL (Time to Live), ToS (Type of Service), IP Checksum, TCP Sequence Number, TCP Checksum, TCP Flags, ICMP Checksum, UDP Checksum, ICMP Message Type, DNS Query, DNS Query ID, HTTP request URI
<b>Bandwidth Management</b>	Guarantee bandwidth per application (granular, per user or session basis). Limit bandwidth per application. Limit P2P protocol traffic per session.
<b>IPv6</b>	Support IPv6 networks and block IPv6 attacks.
<b>Access Control</b>	Access Lists, Black/White Lists
<b>Alerting</b>	SNMP, Log File, Syslog, E-mail
<b>Forensics</b>	Attack Packet Logging, In-depth Attack Footprint Analysis, Attack details and statistics
<b>Management</b>	SNMP V1, 2C, 3, HTTP, HTTPS, SSH, Telnet, Console
<b>Availability</b>	Fail-Open Bypass: Internal for copper ports, external for fiber ports. Dual Power Ready. Advanced Overload mechanism maintaining maximum security coverage under extreme traffic load.
<b>Physical</b>	
Dimensions (W x D x H) mm	440x484x88
Weight (lb, kg)	14.52 lb, 6.6 kg
Power Supply	Auto range: 100V-120V/200V-240V AC 50-60Hz or 38-72VDC
Power Consumption	110.8W
Heat Dissipation (BTU/h)	378.32 BTU/h
Operating Temperature	0-40C
Humidity (non-condensing)	5% to 95%
Safety Certifications	EN 60950, UL 1950, CSA 22.2 No. 950
EMI	EN 55022, class B, EN 55024, FCC, part 15B, class B
<b>Warranty</b>	1-year hardware and software maintenance
<b>Support</b>	Certainty Support Program

(1) Actual performance figures may change per network configuration, traffic type, etc.

(2) With DoS Shield and behavioral DoS features; max 2,000,000 concurrent sessions with SYN Cookies and BWM features.

Specifications subject to change without notice.