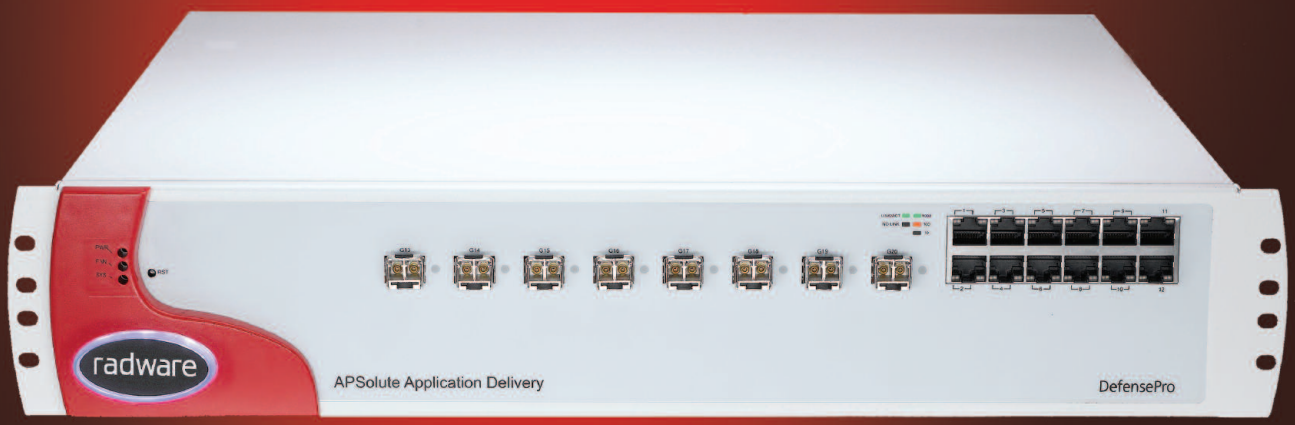

Radware DefensePro-x02 and x20

Multi-layer Intrusion Prevention and DoS Protection, Up to 3 Gbps

From the core to the perimeter, Radware DefensePro provides your enterprise with comprehensive intrusion prevention, behavioral anomaly detection and denial of service (DoS) protection from a wide variety of known attacks and unknown, zero-day attacks. Protecting against worms, viruses, spyware, pre-attack probes and other threats, this easy-to-use, scalable solution proactively prevents both network- and application-level attacks while ensuring high performance for legitimate application traffic, even when under attack.

Lower risk, higher performance, and improved TCO

Radware DefensePro integrates multiple layers of security, including signature-based protection, protocol anomaly protection, encrypted SSL attack protection, access control and bandwidth management. Moreover, it is the industry's first solution to fully integrate adaptive, behavior-based protection capabilities to provide unparalleled security. The solution employs adaptive behavioral analysis to immediately identify and mitigate a wide range of threats – including zero-day attacks - without requiring human intervention.

DefensePro's customized, ASIC-based hardware architecture ensures the highest levels of security, availability and performance. The DefensePro-x20 series supports multiple segments for monitoring enterprise core and perimeter environments. The DefensePro-x02 series for single segment monitoring offers the best price-to-performance for securing the enterprise perimeter, departments and remote branches.

Software-based performance upgrades maximize investment protection, allowing you to scale your solution easily and affordably by simply purchasing a software license for greater thruput. The DefensePro-x20 series scales from 600 Mbps up to 3 Gbps; the DefensePro-x02 series scales from 100 Mbps to 1 Gbps.

A solution that "self-learns" at lightning speeds

DefensePro's behavior-based, self-learning mechanism proactively scans for anomalous network traffic patterns. When detecting an attack, DefensePro characterizes the attack's unique behavior, establishes filter criteria and executes the appropriate countermeasures. A closed-feedback mechanism dynamically modifies filtering criteria as the attack unfolds, protecting against even the most sophisticated attacks with a high degree of accuracy.

Ensuring application continuity during an attack

End-to-end bandwidth management enables dynamic traffic shaping. This proactively isolates the impact of an attack, prevents its spread, and guarantees bandwidth and service levels for critical applications.

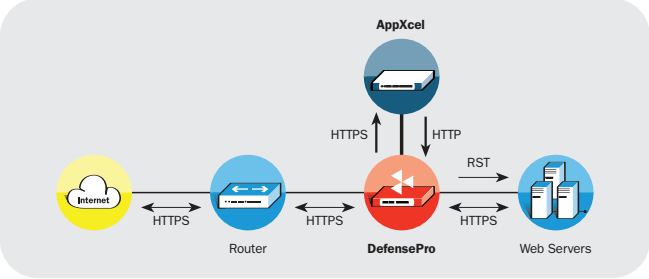

Figure 1: SSL Attack Protection

Unlike competitors' solutions, DefensePro provides a high level of protection against encrypted SSL-based attacks that would otherwise evade security inspection.

radware

DEFENSEPRO FEATURES

The Most Comprehensive Set of Protection Mechanisms

Full application security for the enterprise and data centers

DefensePro's multi-layer protection includes web protection against IIS and Apache vulnerabilities, SQL injection and cross-site scripting; mail server protection against POP3, IMAP and SMTP vulnerabilities; SQL servers and DNS service protection against SQL and DNS vulnerabilities; remote access protection against Telnet and FTP server vulnerabilities; and protection against brute force and backdoor attacks.

Protection against encrypted, SSL-based attacks

In conjunction with Radware's AppXcel Application Accelerator appliance, DefensePro provides a powerful and scalable solution for protection against encrypted SSL-based attacks that would otherwise evade regular security inspection. (See Figure 1.)

While the original SSL tunnel is maintained between the client and the server, DefensePro copies the SSL traffic to an AppXcel device, which decrypts the traffic and forwards it for inspection to DefensePro. When an attack is detected in the decrypted SSL traffic, DefensePro terminates the malicious session in real time.

Advanced, multi-layer Dos/DDoS flood protection

Protection is provided against both known attacks and unknown zero-day attacks. DefensePro protects against DoS attacks caused by a single packet or several packets, such as buffer overflows, Ping of Death, and Land attacks. In addition, adaptive behavior-based DoS protection mitigates zero-day DoS/DDoS attacks. (See Figure 2.) Known and unknown flood attacks that are blocked include:

- DHCP
- TCP SYN/TCP PSH
- TCP RESET
- TCP FIN
- UDP/ICMP/IGMP flood attacks

Inline, stateful, deep packet inspection

DefensePro combines powerful features - bi-directional, stateful, deep packet inspection and accelerated, multi-gigabit-speed signature matching for thousands of attack signatures - to immediately block worms, viruses, Trojans and intrusions. DefensePro also provides protection from brute-force attacks, backdoors and spyware.

Stateful inspection for protocol anomalies (L4-L7)

DefensePro protects against protocol misuse with RFC compliance verification. IP Defragmentation and TCP reassembly help overcome evasion techniques.

Proactive prevention of network scanning and pre-attack probes

Prior to launching an attack, hackers often look for open application ports on network servers or available machines on a service port. DefensePro detects and mitigates scanning activity that threatens to compromise your mission-critical systems. Reconnaissance protection capabilities include mitigation of known scanning tools and all types of port scanning, including horizontal scans, vertical scans and ping sweeps.

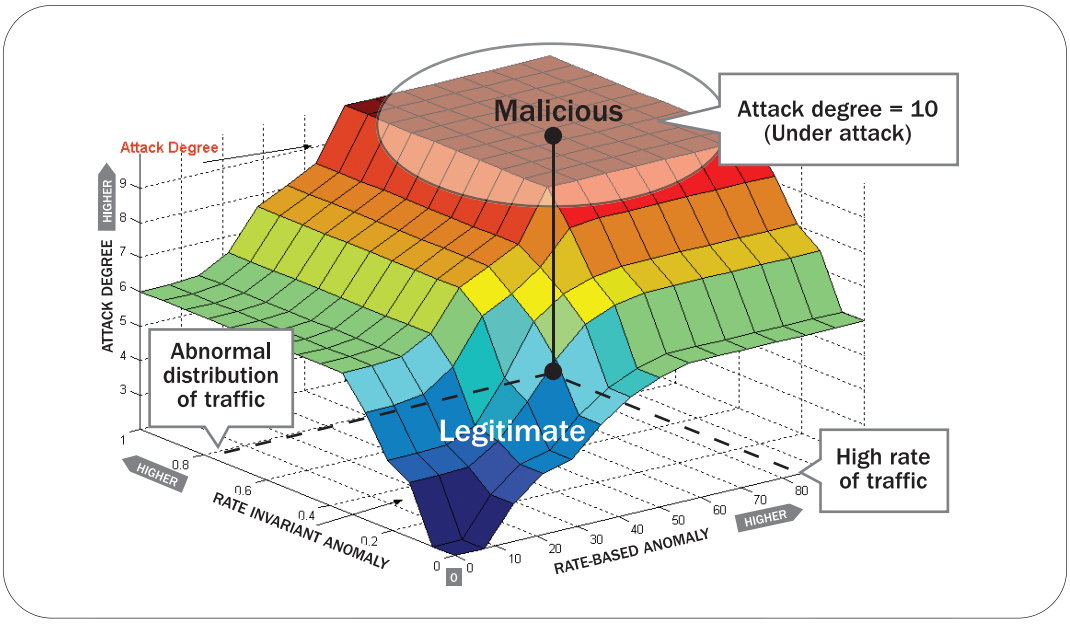

Figure 2: Blocking Malicious Traffic

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

Bandwidth management and access control for end-to-end traffic shaping and optimization

DefensePro's Bandwidth Management and Access Control modules enable dynamic control of bandwidth from end to end. This makes it possible to isolate attacks and prevent their spread while ensuring the continuity of mission-critical applications. Bandwidth can be limited per client or per session. Access control of traffic, per application ports, hosts and networks, allows only predefined application traffic.

For example, controlling the bandwidth usage of peer-to-peer (P2P) applications ensures adequate bandwidth for legitimate application traffic while also reducing the propagation of worms and viruses via P2P applications.

Security updates

With Security Update Service, Radware's 24x7 Security Operations Center (SOC) provides subscribers with automated, weekly delivery of new attack signature filters as well as emergency delivery of filters. This helps ensure networks and applications are fully protected from current and emerging vulnerabilities.

Hardware Architecture

The industry's first software-scalable thruput licensing

DefensePro allows users to increase thruput without a hardware upgrade, providing unparalleled investment protection. The DefensePro-x02 series offers software thruput upgrades from 100 to 200, 500 and 1000 Mbps. The DefensePro-x20 allows software thruput upgrades from 600 Mbps to 1 Gbps and 3 Gbps. (See Figures 3 and 4.)

Figure 3: DefensePro-x02
The DefensePro-x02 series offers the best price/performance for monitoring the enterprise perimeter, departments and remote branches.

Figure 4: DefensePro-x20
The DefensePro-x20 series provides the industry's best price/segment for multi-segment monitoring of the enterprise core and perimeter environments.

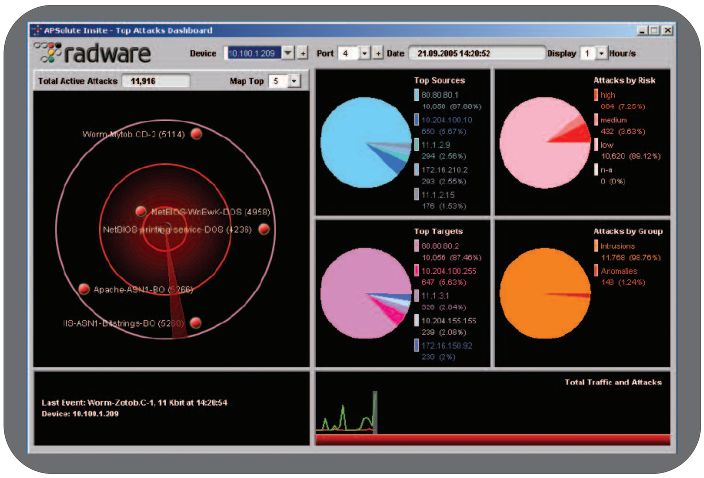

Figure 5: Administrator Dashboard
A real-time dashboard provides administrators with immediate awareness and insight into an attack, so they can respond quickly and effectively.

State-of-the-art, ASIC-based hardware architecture

DefensePro's customized, ASIC-based hardware architecture ensures unmatched security and performance. The system delivers multi-gigabit, real-time thruput and provides the industry's highest port density, enabling protection of up to 9 network segments with a single device.

Redundancy and high availability

DefensePro's built-in internal bypass feature ensures high network availability in the event of hardware (i.e., power) and software malfunctions. A dual power supply provides automatic failover if the primary power supply fails. (The dual power supply is only available for the DefensePro-x20 series.)

Management

Security management and reporting

With features that enable centralized device configuration, monitoring and reporting, Radware's APSolute Insite[1] management solution increases visibility and control of network security. APSolute Insite offers:

- The ability to customize security policies for each network segment.
- A real-time dashboard that enables administrators to monitor attempted attacks, including top sources and destinations and vulnerable resources. (See Figure 5.)
- Pre-defined and customized executive reporting capabilities to support security decision-making and investments.
- Advanced forensics for examining historic network activity down to the packet level.

[1]Available as a DefensePro option.

DefensePro	DP-3020	DP-1020	DP-620	DP-1002	DP-502	DP-202	DP-102
Software/Hardware							
DefensePro software version	3.0 & higher	3.03 & higher					
ASIC-based hardware platform	Application Switch 4 (DP-x20 Series)			Security Platform 1 (DP-x02 Series)			
Performance[1]							
Maximum thruput	3 Gbps	1 Gbps	600 Mbps	1 Gbps	500 Mbps	200 Mbps	100 Mbps
Maximum concurrent sessions	1,600,000[2]	1,600,000[2]	1,600,000[2]	140,000	140,000	140,000	140,000
Latency	< 200 microseconds						
Ports							
GE (GBIC)	8	8	8	-	-	-	-
10/100/1000 copper	12	12	12	3	3	3	3
Console RS-232C	Yes						
Scanning Ports							
Maximum segments	9	9	9	1	1	1	1
Network operation	Transparent L2 Forwarding						
Management Ports	Includes GE, FE and RS-232						
Memory (Main CPU RAM)	512MB	512MB	512MB	512MB	512MB	512MB	512MB
Physical							
Dimensions (w x d x h) mm	432x455x88	432x455x88	432x455x88	298x215x44	298x215x44	298x215x44	298x215x44
Weight (lb, kg)	15.4, 7.0	15.4, 7.0	15.4, 7.0	4.785, 2.175	4.785, 2.175	4.785, 2.175	4.785, 2.175
Power supply	Auto range: 100V-120V/200V-240V AC 50-60Hz or 38-72VDC			Auto range: 100V-120V/200V-240V AC 50-60Hz			
Power consumption	108W	108W	108W	20W	20W	20W	20W
Heat dissipation (BTU/h)	368.758	368.758	368.758	68.3	68.3	68.3	68.3
Operating temperature	0-40C						
Humidity (non-condensing)	5% to 95%						
Deployment Operation Modes	In-line, SPAN Port Monitoring and Copy Port						
Operation Modes	Block and Report, Report Only						
Intrusion Prevention	Web Protection, Mail Servers Protection, FTP Servers Protection, DNS Vulnerabilities, Cross-Site Scripting, SNMP Vulnerabilities, Worms and Viruses, Brute Force Protection, SQL Injections, Backdoors and Trojans, Spyware, Custom Attack Signatures, LAN Protocol and Services Protection (RPC, Netbios, Telnet etc.), Generic Payloads (Remote Execution, Shellcodes)						
Stateful Operation	TCP Reassembly, IP Defragmentation, Access Lists, Black/White Lists						
Signature-based Protection	Support up to 65,000 User-defined Signatures. Real-time Signature Updates provided.						
Anomaly-based Prevention	L4-L7 Stateful Protocol Anomalies						
Reconnaissance Detection	Scanning Tools, Horizontal and Vertical Scanning, Stealth Scanning, Backdoors and Trojans, Ping Sweeps						
DoS/DDoS Protection[3]	Adaptive Behavior-based, Zero Day protection. Flood Protection for SYN, TCP, UDP, UDP (with ICMP Back Scattering), DNS Query, ICMP, IGMP, IP Fragment Floods. TCP Connection Flood Protection, and high rate self-propagating network worms						
Attack Isolation	Guarantee bandwidth per application (granular, per user basis). Limit bandwidth per application. Limit P2P protocol traffic per session.						
SSL Attacks Prevention	Available for DP-3020, DP-1020 and DP-620 in conjunction with AppXcel						
Attack Prevention Mechanisms	Block attacks in real time with: Adaptive Smart Dynamic Filters, Proxy-based SYN Cookies, TCP Connection Resetting, Connection Blocking, Dynamic Source IP Blocking, Connection Rate Limit, Actions per Attack						
Packet Filter Criteria (Adaptive Smart Dynamic Filters)	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						
Alerting	SNMP, Log File, Syslog, E-mail						
Forensics	Attack Packet Logging, In-depth Attack Footprint Analysis						
Management	SNMP V1, 2C, 3, HTTP, HTTPS, SSH, Telnet, Console						
Availability	Fail-Open Bypass: Internal for copper ports for all models. External for fiber ports available for DP-3020, DP-1020 and DP-620. Dual Power Ready for DP-3020, DP-1020 and DP-620						
Warranty and Support							
Warranty	1-year hardware and software maintenance						
Support	Certainty Support Program						

[1] Actual performance figures may change per network configuration, traffic type, etc.
[2] 1,600,000 sessions supported with 1024MB memory. 550,000 sessions supported with 512MB.
[3] Bundled for DP-102, DP-202, and DP-502. Optional module for DP-1002, DP-620, DP-1020, and DP-3020.
Technical specifications and product information are subject to change without prior notice.