DefensePro: DDoS Protection and Attack Mitigation

Protect the Data Center and Network Against Emerging Network Threats

In today's info-security threat landscape, denial of service and distributed denial of service (DoS/DDoS) attacks are a major cause of network downtime. Whether executed by hacktivists to draw attention to a cause, fraudsters trying to illegally obtain data or funds, or a result of geo-political events, DDoS attacks are a destructive cyber weapon. Governments, utilities, financial services and commercial institutions face daily attacks.

Attacks are becoming more sophisticated and increasing in severity as they bypass traditional cloud and CDN protection services to target an organization's IT infrastructure and critical applications.

The simplicity of launching cyber-attacks and variety of attack tools available are reasons why organizations suffer from increased attacks, such as DDoS. It is no longer about preventing attacks, but rather how to detect and mitigate them.

What Does DefensePro Do?

DefensePro is part of Radware's attack mitigation solution and is an award-winning, real-time, perimeter attack-mitigation device that secures organizations against emerging network and applications threats. DefensePro protects the infrastructure against network and application downtime (or slow time), application vulnerability exploitation, malware spread, network anomalies, information theft and other types of attacks.

DefensePro helps organizations win the ongoing security battle against availability attacks, by detecting and mitigating known and zero-day DoS/DDoS attacks in real-time. It protects against other security threats that are usually undetected by traditional DDoS mitigation tools, such as SSL-based flood attacks, attacks on login pages and attacks behind CDNs.

With DefensePro, Radware's attack mitigation solution offers protection with the shortest mitigation time and broadest attack coverage. Radware provides a hybrid solution combining on premise and cloud-based mitigation tools in a single integrated solution, designed to optimally block multiple attack vectors occurring in parallel.

Why DefensePro?

DefensePro includes a comprehensive set of four essential security modules – anti-DDoS, network behavioral analysis (NBA), intrusion prevention system (IPS) and SSL attack protection (DefenseSSL) - to fully protect the application infrastructure against known and emerging network security attacks. It employs multiple detection and mitigation modules including adaptive behavioral analysis, challenge response technologies and signature detection.

DefensePro Advantages

- Network Behavioral Analysis (NBA), Intrusion Prevention System (IPS) and SSL Attack Protection (DefenseSSL)
- Up to 350Gbps throughput inspection
- Mitigates up to 330M PPS of attack traffic while preserving best quality of experience
- Up to 18M concurrent sessions

Compared to stand-alone solutions, the synergy of multiple security modules on a single, hardware-accelerated platform enables more effective protection against attackers who seek to systematically compromise business assets while providing unified reporting, forensics and compliance.

DefensePro consists of patent protected, adaptive, behavioral-based real-time signature technology that detects and mitigates emerging network attacks, zero-minute, DoS/DDoS, application misuse attacks, network scanning and malware spread. It eliminates the need for human intervention and does not block legitimate user traffic.

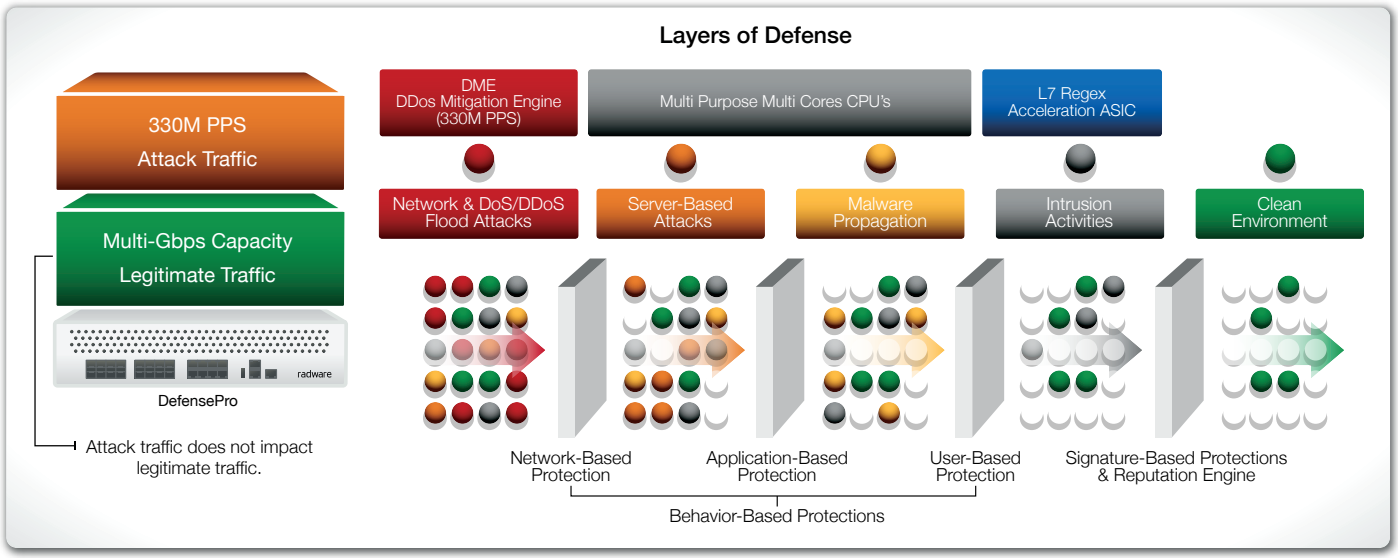

Figure 2: DefensePro Architecture

Deployment Modes

DefensePro devices can be deployed inline, out-of-path (OOP) or in a scrubbing center to provide the highest mitigation accuracy within the shortest time. Each deployment mode offers the same performance as an inline device.

With DefensePro deployed either inline or out-of-path as well as in a scrubbing center, the devices are able to communicate with each other in real-time to collect automatic updates of normal traffic baselines, detect behavioral patterns and obtain attack footprints. This constant real-time flow of defense messaging enables DefensePro to provide accurate and instant mitigation without the need to learn this information when an attack occurs.

Deploying DefensePro devices out of path or in a scrubbing center is the most scalable and flexible solution as it is based on the maximum attack mitigation capacity needed, without being limited by the actual network physical topology.

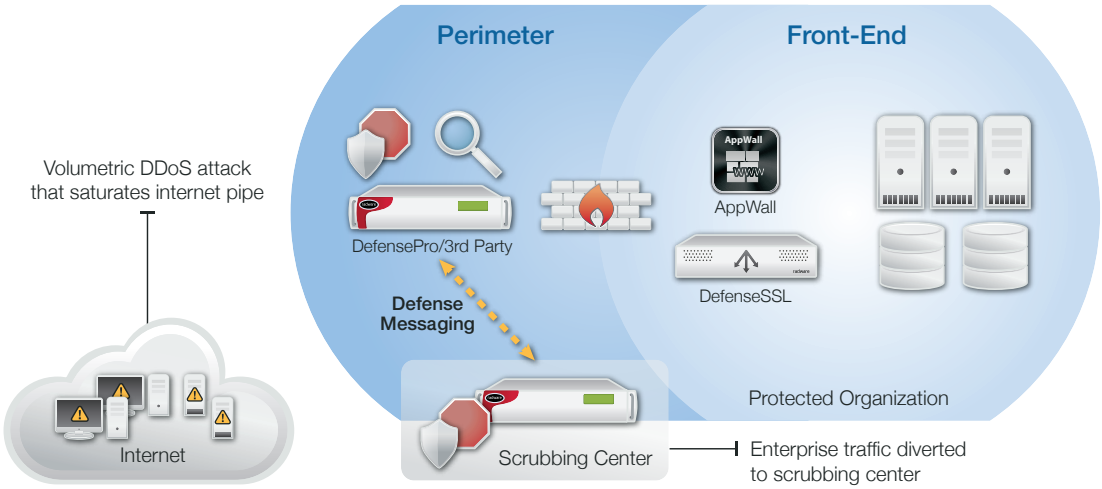

Figure 3: DefensePro device deployed inline in the enterprise perimeter to detect/mitigate attacks in real-time; scrubbing center invoked for mitigation of volumetric attacks that threaten to saturate the internet link.

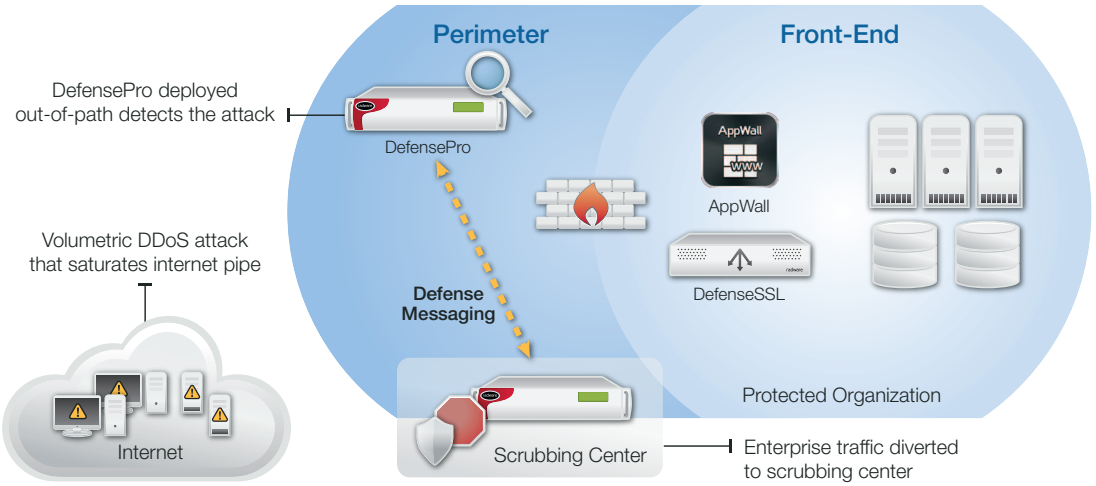

Figure 4: DefensePro deployed out-of-path for attack detection; suspicious traffic is diverted to the deployment with scrubbing center for attack mitigation.

Fits Your Needs

DefensePro is offered both as a physical appliance and as a virtual appliance to fit your needs. The DefensePro series of physical appliances offers versatile connectivity and mitigation capacities, adhering to enterprise and service provider deployments. DefensePro is also available as a virtual appliance, DefensePro VA, which provides the flexibility in protection needed in a few key scenarios:

- Allows enterprise customers that are based on a Software Defined Data Center (SDDC) architecture to include DDoS mitigation capabilities based on a virtual DDoS mitigation appliance. DefensePro VA fully integrates into SDDC architecture supporting various virtualization technologies and enabling easy provisioning, automation and orchestration.

- Enables cloud providers to offer Top-of-Rack DDoS mitigation services to hosted applications, by smoothly integrating with their cloud orchestration and management systems.

- Used by carriers and service providers as part of their offering for managed vE-CPE services, inter-operating with various MANO (management and orchestration) solutions.

Integrated, Hybrid Solution

In addition to the security modules integrated in DefensePro, Radware's attack mitigation solution includes an SSL decryption/encryption engine, a WAF module and Hybrid Cloud DDoS Protection Service that works in sync with the on premise solution. With no performance impact or risk, Radware's attack mitigation solution ensures business continuity even when under attack.

The solution is enhanced with a central Security Information Event Management (SIEM) to provide unified situational awareness and Radware's Emergency Response Team (ERT) offering of 24/7 security expert support for customers under attack in real time to mitigate attacks and restore operational status.

Unique messaging assures that each component provides information about traffic baselines and real-time signatures to the others, so that all system components have full visibility into all information.

Through this messaging, Radware's attack mitigation solution can detect attacks where it should and mitigate attacks where it's best. For example, the system can detect a volumetric attack at the network perimeter but mitigate it in the cloud. This automatic, real-time feature enables organizations to scale the mitigation capabilities of the solution by moving mitigation as far as possible from the application infrastructure.

Business Value

Maintain Business Continuity of Operations (COOP) Even When the Network is Under Attack

- Full protection of data center applications against emerging network threats
- Maintain network performance even when under high PPS network attacks
- Maintain excellent user response time even under attack

Best Security Solution for Data Centers in a Single Box

- DefensePro combines intrusion prevention system (IPS), network behavioral analysis (NBA), denial-of-service (DoS) protection and DefenseSSL
- Get the most accurate attack detection and prevention without blocking legitimate user traffic

Reduce Total Cost of Ownership (TCO) of Security Management

- Multitude of security tools in a single box
- Single management application to manage multiple DefensePro units cross multiple data centers
- Full investment protection and extended platform life time with pay-as-you-grow license upgrade scalability delivering best ROI and CAPEX investment protection

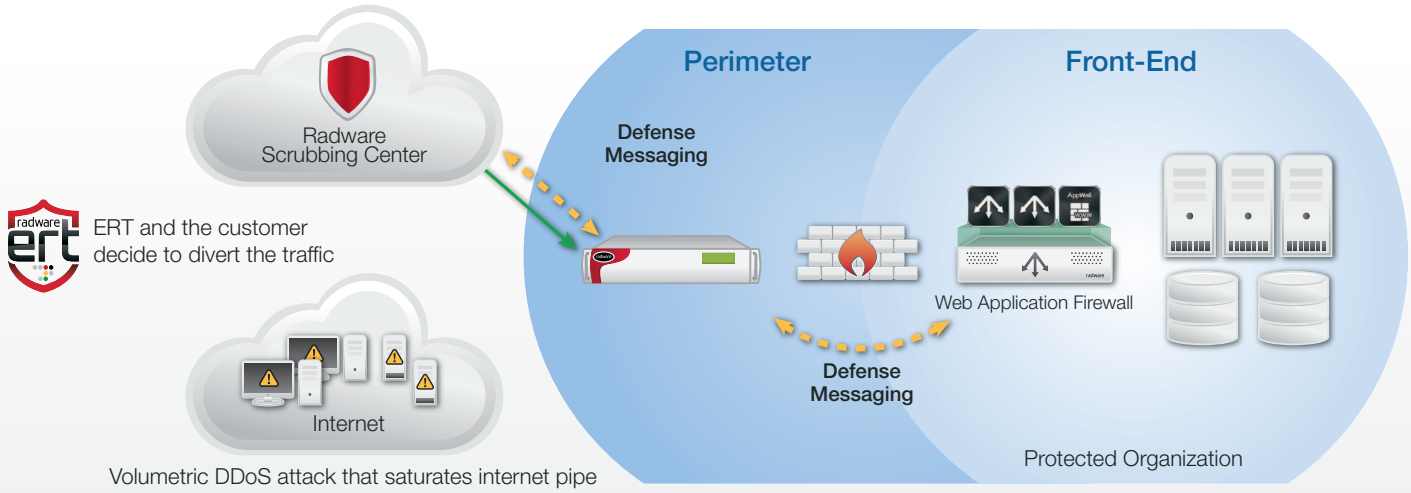

Figure 5: Complete Attack Mitigation Solution Deployment

Benefits

Widest Attack Coverage with detection and mitigation of the following attack types:

- Known and zero-day DoS/DDoS flood attacks that misuse network bandwidth resources
- Application DoS attacks that misuse server and application resources including:
  - HTTP/HTTPS and DNS flood attacks
  - SIP scans and flood attacks
  - Web stealth attacks (e.g., Login page brute force attacks, SSL-based attacks)
  - Information theft – application scanning
- Application vulnerability attacks that exploit server application weaknesses including Web, Mail, DNS, FTP, SQL server vulnerabilities
- Offered as a physical or virtual appliance to best fit the unique needs of your organization.

High Performance

- Up to 350Gbps throughput inspection
- Block high packets-per-second (PPS) attacks that overuse the CPU resources of your networking and security equipment up to 330M PPS
- Attack mitigation solution that can be deployed both inline and out-of-path, maximizing scalability and flexibility
- Granular challenge/response technology for detecting advanced Botnets which imitate legitimate users; maintaining the highest response time for legitimate users

Technical Specifications and Requirements

For additional information regarding technical specifications or requirements please refer to Radware's Tech Specs for:

DefensePro x4420 Series
DefensePro x420 Series
DefensePro x412 Series
DefensePro x06 Series
DefensePro VA Series

About Radware

Radware® (NASDAQ: RDWR), is a global leader of application delivery and cyber security solutions for virtual, cloud and software defined data centers. Its award-winning solutions portfolio delivers service level assurance for business-critical applications, while maximizing IT efficiency. Radware's solutions empower more than 10,000 enterprise and carrier customers worldwide to adapt to market challenges quickly, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

Radware encourages you to join our community and follow us on: Facebook, Google+, LinkedIn, Radware Blog, SlideShare, Twitter, YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis on DDoS attack tools, trends and threats.

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 & security solutions can enable you to get the most of your business and IT investments, email us at info@radware.com or go to www.radware.com.

PRD-DP-DS-04-2016/09 - US