FAST, ACCURATE DDOS ATTACK DETECTION WITH SCALABLE MITIGATION

Kentik Detect combined with the Radware Attack Mitigation System delivers an integrated solution to leverage network data analysis and scalable mitigation for effective DDoS attack protection, on-premises or in the cloud.

The Challenge

Denial of service and distributed denial of service (DoS/DDoS) attacks continue to increase in frequency, complexity and size, forcing enterprises and service providers to evaluate the scope, accuracy and scalability of their protections.

The Solution

Kentik and Radware have partnered to provide an advanced DDoS detection, orchestration and mitigation solution that protects enterprises and service providers from DDoS attacks, botnets, and zero-day attacks.

Benefits

Leverages network traffic analytics to provide the widest security coverage, reduced operational costs, increased attack visibility and the value of an out-of-path DDoS attack mitigation solution.

DDoS attacks have become a major threat. Hacktivism, ransom and other cyber crimes have become so prevalent that every online business, financial service, government agency, public utility or service provider is now a target. As DDoS attacks become increasingly complex, attackers are deploying multi-vector attack campaigns that target every layer of the application infrastructure (network, server and enabling services such as DNS). Attackers then move to the application layer, exhausting server and application resources using stealth attack techniques or encryption that evade detection by traditional security tools.

Enterprises and service providers alike benefit from the Kentik/Radware collaboration with a cost effective, flexible DDoS detection and mitigation solution that protects network and application infrastructure from an array of malicious attacks. The solution leverages two best-of-breed solutions in the market to provide coordination across attack detection, orchestration and mitigation.

Detection

Kentik Detect provides complete visibility into network traffic anomalies, including both alerting and full-resolution drilldown on raw flow records, enabling operators to respond rapidly and effectively to each DDoS threat. Kentik Detect ingests multiple types of network data (NetFlow/sFlow/IPFIX, SNMP, BGP) at scale and fuses it into a unified data store for full forensic access. Kentik Detect's unlimited access to raw flow records, coupled with the user portal's many flexible analytic pivots, lets operators see, analyze, and understand attacks in detail, so that predefined DDoS alert templates can be extended for automatic recognition and notification of new and changing threats.

Kentik Detect evaluates and raises alerts during real-time data ingest, which means immediate visibility and awareness in the event of an attack. Kentik's alerting system supports flexible notification techniques including email, syslog, and/or JSON/URL.

Orchestration

The optimal strategy for DDoS protection across large networks is to detect where you can and mitigate where you should. Orchestration of attack mitigation means coordinating the use of different mitigation assets on-premises or in the cloud based on the type and size of the attack. The Kentik/Radware solution is able to collect input from distributed detection elements and then aggregate, correlate and analyze in the context of the protected service. It also implements security, availability and scale logic, and applies the optimal action based on the available distributed mitigation components. Orchestration can be implemented via Radware's DefenseFlow and Kentik Detect.

Mitigation

Radware's Attack Mitigation System (AMS) is an integrated system that provides world-class security, including DDoS attack mitigation and SSL-based protection to fully protect applications and networks against all types of availability-based attacks.

The Radware solution supports distributed mitigation and the ability to mitigate attacks at the optimal location utilizing different mitigation components. In this context, optimal means the furthest away from the protected infrastructure with the least disruption of traffic flow and impact on user experience. Mitigation capabilities include usage of the Radware DefensePro, leveraging the network via BGP, real-time black hole (RTBH), BGP Flowspec, and Radware's cloud mitigation solution.

Radware DefensePro is a dedicated hardware accelerated platform that provides attack mitigation at network throughputs up to 300Gbps and up 230M PPS attack prevention rate. Additionally, Radware also offers Cloud DDoS Protection Services, with over 2 Tbps of mitigation capacity across five global scrubbing centers, providing protection against the largest volumetric attacks.

The accuracy and speed of effective mitigation across the entire solution is aided by Radware's Defense Messaging, a proprietary communications method that enables the components of the Radware AMS to share normal traffic baselines, security policies and attack profiles. Defense Messaging supports Radware's unique single-vendor solution that streamlines coordination and improves mitigation accuracy, and ensures the same technology is applied to mitigation either on-premises or in the cloud.

Solution Benefits

- Maintain business continuity of operations when under attack. The joint solution offers the widest coverage against all types of availability-based threats that target service provider networks and enterprise applications.
- Reduced operational costs and increased attack visibility due to a highly granular centralized monitoring and control system.
- A cost effective DDoS protection solution with flexible deployment options (out-of-path, cloud).
- Attack mitigation coordination to ensure use of optimal mitigation resources based on attack type, attack size, or assets being protected.

Unique Capabilities of the Kentik/Radware Joint Solution

- Accurate attack detection: Kentik Detect uses deep flow-based monitoring to detect DDoS attacks that bypass firewalls and IPSs.

- A highly scalable solution - the Radware DefensePro provides 300Gbps of network throughput and up to 230 million packets-per-second (PPS) attack scrubbing per appliance and can be scaled linearly with multiple appliances.

- Advanced management through the Kentik Portal that provides a single unified environment for all sources and types of network data (NetFlow, SNMP, BGP, etc.) and monitoring and reporting of DefensePro security events.

- Most accurate and scalable attack mitigation solution in the industry with Radware Attack Mitigation System.
  - Hardware accelerated mitigation of all network DDoS flood attacks using behavioral based real-time signatures
  - Behavioral-based application DDoS attack mitigation using accurate L7 footprint
  - Hardware accelerated DPI engine blocking low and slow attacks and known tools such as Slowloris, RUDY, LOIC and many more
  - Non-intrusive, asymmetric SSL attack mitigation
  - Shortest time to protect – within seconds

Learn More About Our Integrated Solution

If you would like more information about the joint solution from Kentik and Radware, please contact radware_kentik@radware.com.

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.