PROTECTING AGAINST CRITICAL AND DESTRUCTIVE INFRASTRUCTURE DDOS ATTACKS

It is assumed that Distributed Denial of Services (DDoS) attacks on the critical infrastructure of the utilities operational network may have devastating results. With the right conditions and timing, attackers can create an attack that is much more destructive than recent web events. Radware's Attack Mitigation System (AMS) offers the broadest coverage for DDoS attacks that involve minimal time to mitigate.

Challenge
Denial of Service/Distributed Denial of Service (DoS/DDoS) attacks on the operational network will have devastating results. Attacks are becoming more sophisticated using multi-vulnerabilities, on different layers of the infrastructure.

Solution
Radware offers enterprises an Always On hybrid DoS/DDoS mitigation solution, with the broadest attack vector mitigation solution against multi-vulnerabilities attacks.

Benefits
Attack Mitigation System offers an Always On DoS/DDoS mitigation solution with minimal time-to-mitigate and broadest attack coverage. This provides organizations a solution that stops multi-vulnerability DDoS attacks instantly.

With the move from SCADA based networks to IP based Smart Grid networks, utility companies are becoming more concerned with operational Distributed Denial of Service (DDoS) attacks. The impact of a successful DDoS attack can be catastrophic. Disabling a power station and causing millions of people to be without electricity for several hours is incomparable to the damage that other Internet attacks have caused. There is no other cyber attack for which the impact can threaten the environment in such magnitude.

Regulators all over the world are working on new specifications to prevent DDoS attacks on critical infrastructures. The increased regulation activity has included the North American Electric Reliability Corporation (NERC), the Federal Energy Regulatory Commission (FERC) and Presidential Security Order 13636 in the states. Similar regulations exist almost in every country around the world.

As attacks on critical infrastructures are considered an act of war, it is assumed that when such an attack takes place, the attacker party (usually another country or large criminal organization) has plenty of resources to plan and deploy sophisticated and devastating attacks. While the roots of DoS and DDoS attacks are planted at the dawn of the Internet, sophisticated DDoS attacks have become very popular in the last couple of years. In attacks that are hard to defeat, attackers are using multi-vulnerability attack campaigns, running different attack vectors in parallel and targeting multiple vulnerability points at the victims IT or operational infrastructure in different layers of the organizational infrastructure including network, servers and applications. This may cause a utility company to be at a higher risk, as only one attack vector needs to successfully hit the target in order for the result to be destructive. The attackers' assumption is that even if the victim deploys multiple protection tools, there are blind spots in the perimeter network security architecture and therefore the victim is exposed to several attack vectors.

Radware Attack Mitigation System

Attack Mitigation System (AMS) is a hybrid solution, combining are an on-premises detection and mitigation solution with cloud-based volumetric attack scrubbing. This combination ensures that all forms and sizes of the attack are dealt optimally and instantly. Hybrid anti-DDoS solutions are recognized by IDC as offering optimal protection against the full gamut of attack vectors that are employed today.

Real-time, Always-On Protection – Minimal Time to Mitigate

DefensePro, Radware's on premise anti-DDoS component, ensures that the data center and the operational network are constantly protected. DefensePro provides Always On, full protection against multi-vector DDoS attacks. Only in cases of volumetric attacks, where the network pipe is about to be saturated, traffic is diverted to DefensePipe. Radware's DefensePipe is a cloud-based scrubbing center, clearing attack traffic before it reaches the company's Internet pipe. It enables a smooth transition between mitigation options.

The Always On protection capability ensures that the organization is fully protected at all times, and time to mitigate is measured in seconds. Moreover, in case of an attack that requires the traffic to be diverted to the cloud-scrubbing center, the protection continues with no destruction or gaps.

Securing SCADA with DefensePro

As organizations still rely on SCADA networks for legacy operational network architecture, it is imperative that DDoS mitigation solutions include protection mechanisms for SCADA networks.

DefensePro offers comprehensive protection for SCADA based networks. This protection includes a signature based protection suite including signatures against known vulnerabilities. Behavioral DoS protection on SCADA and Smart Grid networks ensures protection against zero-day DDoS attacks.

Minimal Impact on Legitimate Traffic

Attack Mitigation System is unique because the on-premise mitigation solution adds no latency to the legitimate traffic. A special hardware based engine mitigates the different attack vectors, ensuring that legitimate traffic is not affected, and network real-time operations is not degraded even during an attack.

Widest Attack Mitigation Coverage

It offers a multi-vector attack detection and mitigation, handling attacks at the network layer, server based attacks, malware propagation and intrusion activities. The solution includes protection against volumetric and non-volumetric attacks, SYN Flood attacks, Low & Slow attacks, as well as application level attacks. As the solution constantly analyzes the traffic, it builds traffic baselines that are customized for the deploying organization. With a unique patented mechanism Radware's solution is capable of automatically creating a real-time signature of the attack, using this signature to mitigate the attack.

Encrypted Attack Protection

Radware' SSL mitigation solution is unique in the industry. AMS mitigates SSL encrypted flood attacks at the network perimeter, with no need to share the SSL private-keys. These private-keys are critical, sensitive information and in some cases cannot be shared with other organizations because of regulation.

AMS mitigates SSL based attacks using unique challenge-response mitigation techniques. SSL decryption and challenge response mechanisms are enforced only on suspicious traffic. The result is the lowest latency SSL mitigation solution in the industry, as legitimate traffic is not affected by the mitigation efforts.

AppWall: Taking Web Application Security to the Next Level

AMS Web Application Firewall (WAF) module, Radware's AppWall secures Web applications and ensures availability by mitigating web application security threats and vulnerabilities. AppWall provides complete web application protection against: web applications, web services, XML and more. The solution provides protection against zero-day attacks.

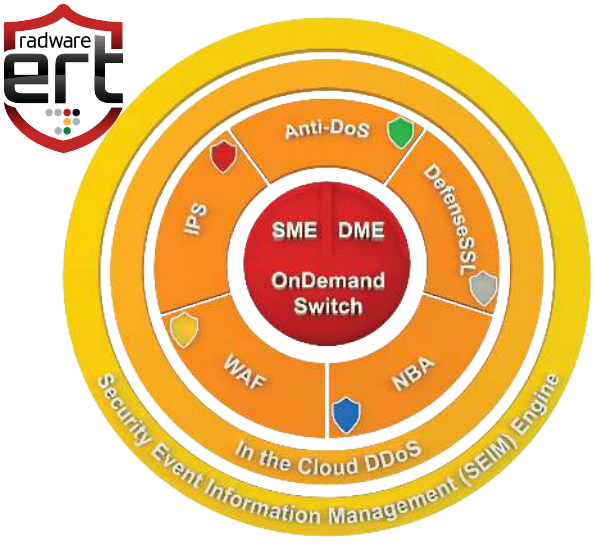

Figure 1: Radware Attack Mitigation System Protection Modules

AppWall includes patented technology to create and maintain security policies for the widest security coverage with the lowest false positives and minimal operational effort. The combination of AppWall with DefensePro, offers the best network and web application security solution for the organization environment.

Built-in SEIM Providing Real-Time Monitoring

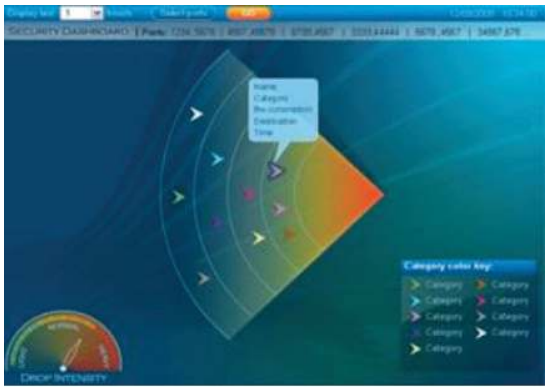

Figure 2: AMS SEIM dashboard view

Built-in Security Event Information Management (SEIM) system provides an enterprise-wide view of security and compliance status from a single console. Data from multiple sources is collected and evaluated in a consolidated view of dashboards and reports. These views provide extensive, yet simple drilldown capabilities that allow users to easily drill into information to speed incident identification and provide root cause analysis, improving collaboration between NOC and SOC teams, and accelerating the resolution of security incidents.

Radware Emergency Response Team – Your Single Contact for DDoS Mitigation Support

Distributed Denial of Service attacks can last a number of hours and can last even days or weeks. In such long intense durations, organizations look for a single point of contact that will help them go through the attack mitigation process, help detect the attack, apply the correct mitigation points at the right time and when needed divert the traffic under attack to the cloud-based scrubbing center.

Radware Emergency Response Team (ERT) provides customers with 24/7 security expert services for hands-on attack mitigation assistance to help successfully defend your network against cyber attacks. ERT provides the required expertise needed during prolonged, multi-vector attacks. This may include working closely with customers to decide on the diversion of traffic during volumetric attacks, assisting with capturing files, analyzing the situation and offering various mitigation options. The ERT is involved in numerous attacks and gains a lot of “combat experience”. This helps other customers in many other ways including sharing attack patterns between customers. The experience the ERT gained from fighting the most known attacks in the industry turned into best practice approaches to fight each and every attack. Radware sums up these efforts in the DDoS tool mitigation recommendations which is available to customers. We also alert customers in case of a concrete attack concerning them.

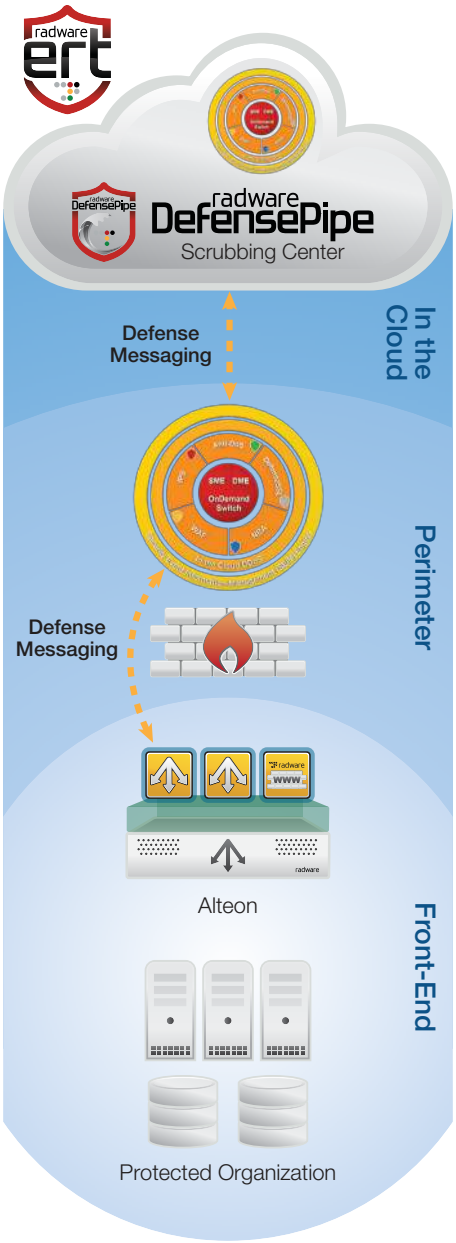

Figure 3: Radware Attack Mitigation Complete Offering

About Radware

Radware (NASDAQ: RDWR), is a global leader of application delivery and application security solutions for virtual and cloud data centers. Its award-winning solutions portfolio delivers full resilience for business-critical applications, maximum IT efficiency, and complete business agility. 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.

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