MITIGATING DDOS ATTACKS IN THE FINANCIAL COMMUNITY

Whether it's a hactivist trying to draw attention, or fraudster trying to illegally transfer funds; the reasons why financial organizations are the target of Distributed Denial of Services (DDoS) are diversified. However the result is always the same. Hundreds of banks and financial organizations around the world are affected from such attacks. Radware's Attack Mitigation (AMS) solution offers the broadest mitigation coverage for DDoS attacks that involve minimal time to mitigate.

Challenge

Denial of Service (DoS)/Distributed Denial of Service (DDoS) attacks are becoming a major reason for infrastructure downtime and service slowness. This downtime causes organizations to lose revenues and increase expenses. DDoS attackers are becoming more sophisticated and are using multiple vulnerabilities attack campaigns.

Solution

Radware offers enterprises an always-on hybrid DoS/DDoS mitigation solution, with the broadest attack vectors mitigation solution against multi-vulnerabilities attacks.

Benefits

Radware's Attack Mitigation System (AMS) offers always-on DoS/DDoS mitigation solution with minimal time-to-mitigation and broadest attack coverage. This provides organizations a solution that stops multi-vulnerabilities DDoS attacks instantly.

Within six weeks in 2013, major banks in the United States experienced 249 hours of downtime caused by Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks. In these long six weeks, banks and financial services public facing web-sites and internal resources either stopped responding or suffered from major degradation in performance.

In an alert to the executives of all United States based banks, as well as any international banks running a service in the US, the Office of the Comptroller of the Currency at the US Department of Treasury (OCC) identified fraud patterns based on DDoS attacks. "Fraudsters use DDoS attacks to distract bank personnel while they gain unauthorized remote access to a customer's account and commit fraud. DDoS attacks also have been used to deny bank customers the opportunity to report suspected fraud and to block the banks' customer-alert communications". The US OCC as well as the European Network and Information Security Agency (ENISA), the Hong Kong Monetary Authority (HKMA) and many other regulators, instruct banks and financial organizations in respected territories to deploy appropriate tools to detect and mitigate the associated risks of DDoS attacks.

While the roots of DoS and DDoS attacks are planted at the dawn of the Internet, recently they have become more complicated, and hard to defeat. Attackers are using multi-vulnerability attack campaigns, that run different attack vectors in parallel and target multiple vulnerability points at the victim's IT infrastructure at different layers of the organizational infrastructure: network, servers and applications. This causes the victims organization to be at 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 a few of the attack vectors. This multi-vulnerability attack campaign was used by Internet activists group Anonymous in Operation Payback in 2010. The attack was against banks as well as other organizations. Since then this technique was used in a large number of attack campaigns, most notably by the Internet hactivist group Cyber fighters of Izz Ad-Din Al Qassam in Operation Ababil. More than 10 different attack vectors were deployed.

Known cyber-attack tactics use DDoS attack vectors to saturate the application security tools (e.g.: Firewall, Intrusion Prevention System) and cause them to stop functioning (i.e.: fail-open). At this point fraudulent activities can take place without interruption. This results in a larger number of attacks, long downtimes and degraded service. In some cases revenues are even lost due to fraud.

Focusing on the Right Mitigation Factors

It is clear that a DoS/DDoS mitigation solution is needed, but what should be the selection criteria for such a solution? Below are key selection factors for choosing a DoS/DDoS attack mitigation solution.

Time to Mitigate: The longer your organization is under attack, the longer your customers, prospects, and internal users suffer from unavailability and slow responses. This results in DoS/DDoS attacks. Consider time to mitigate as a key decision factor for a DoS/DDoS mitigation solution. The sooner the mitigation starts, the sooner your service will be back to normal operation.

Mitigation Coverage: Today's DoS/DDoS attacks are built on a number of attack vectors. More than 50% of Radware customers have experienced attacks with five (5) or more different attack vectors on different layers of the infrastructure. Moreover, in some cases attackers are using DDoS attacks to cover-up other application level attacks. DDoS mitigation solutions should detect and mitigate all of these attack vectors.

About 15% of the attacks organizations experienced involved volumetric attacks that are best mitigated using a cloud-based scrubbing service. A full coverage mitigation solution should be based on a multi-layer approach, where traffic can be diverted to a cloud based scrubbing center in case of a volumetric attack, while other attack vectors are mitigated on-premises.

Single Point of Contact in Case of an Attack: It is crucial that your organization has a single point of contact in case of an attack. This will help the organization choose the correct mitigation options and help the organization divert the Internet traffic between the different mitigation solutions.

Radware Attack Mitigation System

Radware's Attack Mitigation System (AMS) is a hybrid solution, combining on-premise detection and mitigation techniques 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 attacks vectors being employed today.

Real-time Always-on Protection – Minimal Time to Mitigate

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

The 'Always On' protection capabilities ensure that the organization is fully protected 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.

Minimal Impact on Legitimate Users

The AMS solution is unique, in that the on-premise mitigation solution adds no latency to the legit customers' traffic. A special hardware based engine mitigates the different attack vectors, ensuring that legitimate user traffic is not affected, and the user-experience is not degraded even during an attack.

Widest Attack Mitigation Coverage

Attack Mitigation System 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, HTTP floods, SSL based attacks and more. 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 to automatically create a real-time signature of the attack, and use this signature to mitigate the attack where it should be mitigated in the most effective way, either in the scrubbing center in the cloud or on-premise.

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 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 legit 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.

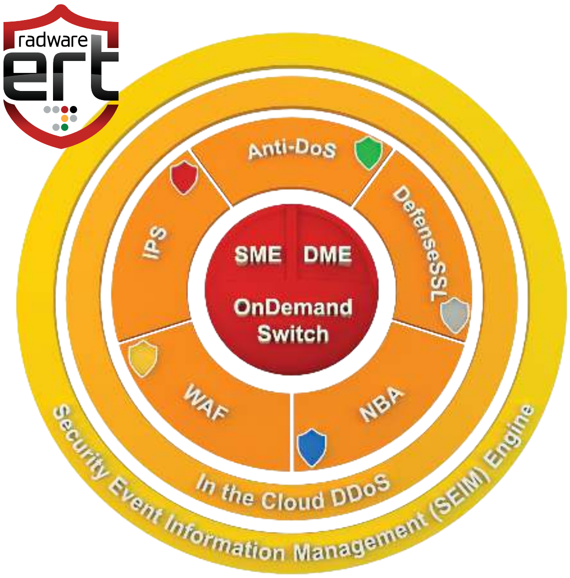

Figure 1: Radware Attack Mitigation System Protection Modules

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's environment.

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. It also provides root cause analysis which improves collaboration between NOC and SOC teams, and accelerating the resolution of security incidents.

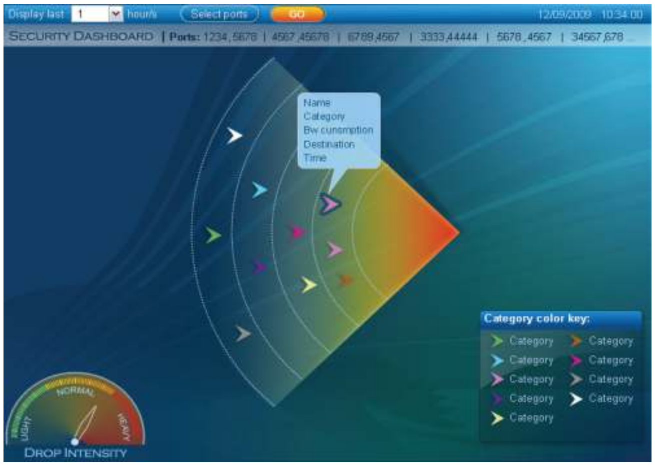

Figure 2: AMS SEIM dashboard view

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

Distributed Denial of Service attacks last a number of hours and can last even days or weeks. In such long intense times, 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 24x7 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 experience helps other customers in many other ways that include sharing attack patterns between customers. ERT experience with fighting the most known attacks in the industry provides 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.

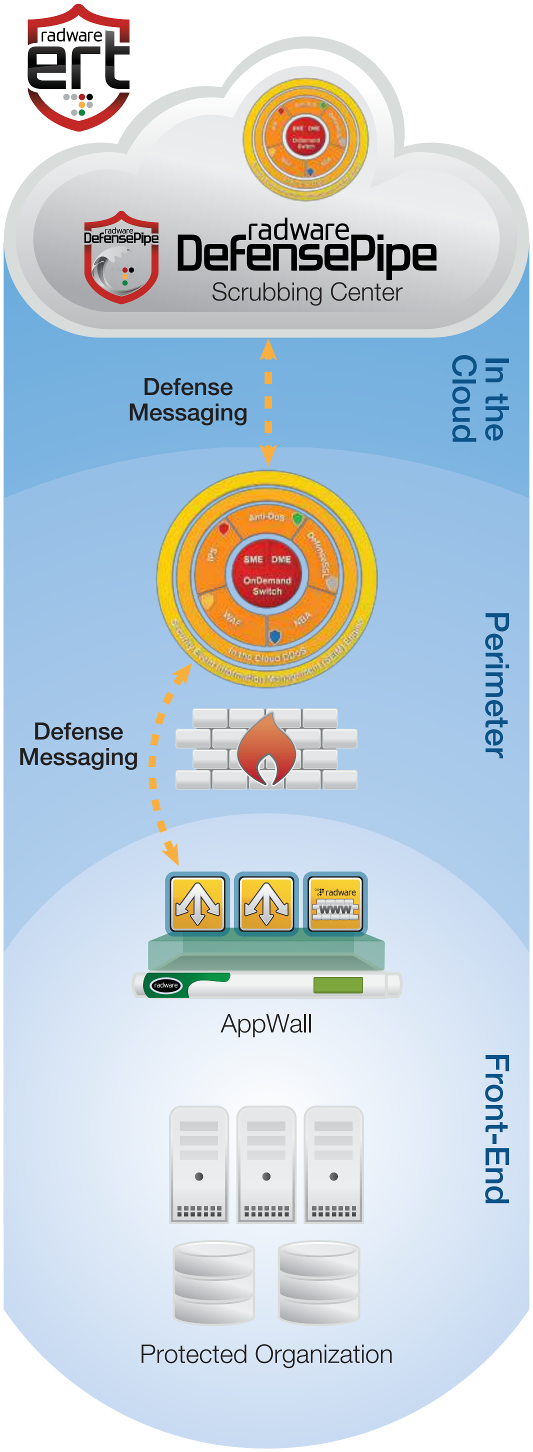

Figure 3: Radware Attack Mitigation

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.