radware

Smart Network. Smart Business.

Securing Online Businesses Against SSL-based DDoS Attacks

Whitepaper

Table of Contents

Introduction

By all indications, 2010 and 2011 will go down in the record books as one of the most active periods of cyber-hacktivism in the history of cyber threats. Moreover, given the current efficacy of hactivist attacks, such as the WikiLeaks revenge attacks (December 2010), South Korean DDoS attacks (March 2011), and NY Stock Exchange DDoS attacks (October 2011, which include a new concept of attacks we define as multi-vulnerability attack campaigns), we believe this will only encouragemore actors to enter the picture and spawn a vicious cycle of future malicious activity.

To demonstrate the rise in frequency of attacks, below is a list of notable attack campaigns that took place over the past 15 months alone:

- December 7th 2010, DoS & DDoS attacks, undertaken by supporters of the WikiLeaks website (group Anonymous), on businesses including MasterCard®, Visa®, PayPal™, the Swedish prosecutor's office, Swiss PostFinance bank, Amazon.com, and others.
- March 4th 2011, DoS & DDoS attack on WorDefenseProress.com severely disrupted operations.
- March 6th 2011, DoS & DDoS attack on Korean e-commerce and government institutions.
- March 6th 2011, attack on the French government's interest in the G20.
- March 9th 2011, group Anonymous declares a new "Operation Payback" against BMI.com and calls for sustained and disabling attacks from its contributing members.
- April 2011, DoS & DDoS attack on Sony's on-line PlayStation® store.
- August 2011, DoS & DDoS attack on the Hong Kong stock exchange.
- October 2011, DoS & DDoS attacks on the New York stock exchange.

Attackers don't rest on their laurels! In the race to be more efficient, and evade detection and mitigation by the existing network security technologies, attackers continue to adapt new attack methods in order to take part in multi-vulnerability attack campaigns. One of these methods is the encrypted DoS & DDoS attacks.

Encrypted DoS Attacks

Online businesses are using cryptographic protocols such as Transport Layer Security (TLS) or its predecessor, Secure Socket Layer (SSL), both of which provide encryption at the application layer to ensure secure end-to-end transit of data.

Attackers are starting to use encrypted SSL DoS & DDoS attacks in order to exploit weaknesses in today's network perimeter defenses.

The main challenges that encrypted DDoS attack present are:

- **Attack impact is higher than clear text attacks**
  Decryption of encrypted data consumes more CPU resources than processing of a clear text. Thus, encrypted application DoS & DDoS attacks amplify the impact, even at relatively low rates of requests per second.

- **Current DoS mitigation technologies don't inspect SSL traffic**
  Today's anti-DDoS security solutions don't support decryption of SSL traffic. Encrypted DDoS attacks are simply passing "under the radar" of existing security solutions.

- **Anti-DoS scrubbing centers are not mitigating SSL based attacks**
  In recent years, increasingly more online businesses adopted the concept of DoS mitigation through "scrubbing centers." One of the main characteristics of these scrubbing centers is that once an attack is detected, only inbound traffic is diverted through the attack mitigation equipment. This asymmetric network condition (i.e., only inbound traffic is seen), presents a serious challenge for the mitigation equipment in decryption of SSL traffic when needed.

- **"In the cloud" anti-DoS managed services don't protect against SSL attacks**
  Anti-DoS managed security services are typically not allowed to store the customers' keys, therefore, they cannot provide the required protection against the encrypted DDoS attack.

There are two main network security product-deployment types that online organizations are using in order to protect themselves against attacks, the in-line approach, and the out-of-path "scrubbing" approach.

The following section describes these two deployment types which are being adopted by online businesses.

Out-of-path Deployment ("Private" Scrubbing Centers)

In high-capacity network environments that require detection and mitigation of large-scale DDoS attacks, a different security approach is usually taken. Instead of using a single network security unit devoted to both detection and mitigation, the detection and mitigation are separated. In these environments, the detector device monitors the traffic, while the mitigator remains idle on a redundant link. Upon attack discovery, the traffic to the network or server under attack is diverted to the redundant path (the scrubbing center). The mitigator device analyzes the traffic, mitigates the attack, and forwards the clean traffic to its destination, using either the regular path or a dedicated tunnel. When the attack ends, traffic diversion is stopped (i.e. the redundant path acts as a temporary mitigation path).

This approach holds several benefits for operators. The most outstanding is its cost-effectiveness; instead of implementing a high-capacity mitigator, or multiple mitigation devices according to the number of physical links, the mitigator device can be a device with lower performance capabilities, since it does not need to inspect all the traffic on the high capacity lines (this is also related to the fact that the scrubbing center needs to handle ingress traffic only). Another benefit to such providers is the possibility to keep their main path clean of DoS attacks, even if the mitigation fails, since it is done on a separate dedicated path.

Radware defines two scrubbing center types, "public" and "private." "Public" scrubbing centers are usually operated by service providers (carrier/ISPs), and provide protection to multiple customers that subscribe themselves to the service. "Private" scrubbing centers are established inside the customer's network. This type is usually used by very large online businesses that take full responsibility for mitigating DDoS attacks that target their own network.

Figure 1-1 below illustrates a "private" scrubbing center network. In this illustration, the attack detection is undertaken by a NetFlow based sensor. Once a DDoS attack is identified, the relevant traffic is diverted through the mitigation equipment inside the scrubbing center. "Clean" traffic is returned to the target servers.

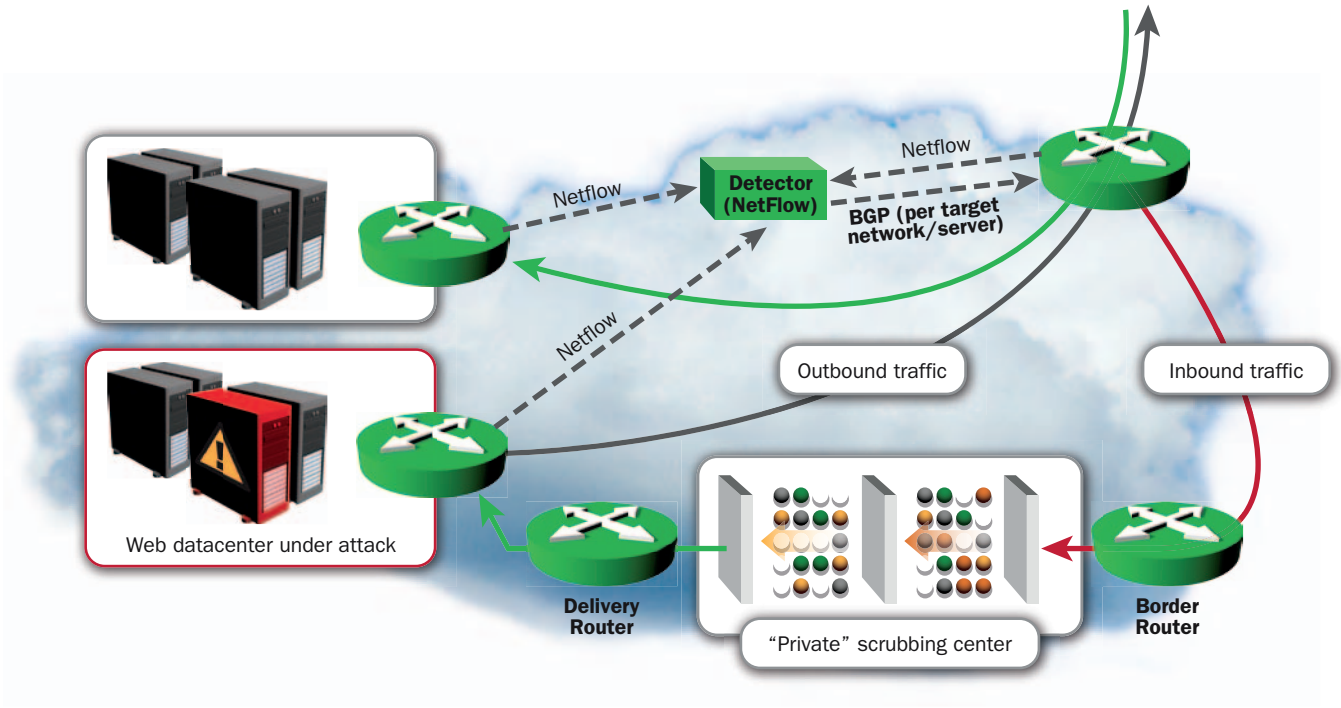

Figure 1-1: Private Scrubbing Center

Mitigation equipment in a scrubbing center must comply with four main requirements:

- **Support asymmetric (ingress only) network**
  The ability to mitigate DoS/DDoS attacks in asymmetric networks(i.e., ingress traffic only).

- **"Zero knowledge" protections**
  The fact that the mitigation equipment "sees" traffic only under attack and not in "peace" time, requires the DoS protections to be able to work effectively without any knowledge of the network and application's normal traffic patterns.

- **Capacity**
  Mitigation equipment of DDoS attacks should be ready to repel very high volumes of attack traffic. Mitigation equipment should be able to block attacks in the scale of multi-million packet per seconds.

- **Encrypted DoS mitigation**

As mentioned before, SSL DoS attacks are beginning to participate in multi-vulnerability attack campaigns. This, together with the fact that many online businesses utilize increasingly more SSL traffic (some large e-commerce sites receive more than 80% of their traffic as SSL traffic), mandates the requirement that the mitigation equipment include SSL DoS attack mitigation capabilities.

In-line Deployment

Lower capacity network environments, or those that require an immediate detection and response capabilities (that cannot be supported by the previous described out-of-path deployment), would prefer an in-line deployment in front of their protected servers.

Figure 1-2 below illustrates an in-line deployment type

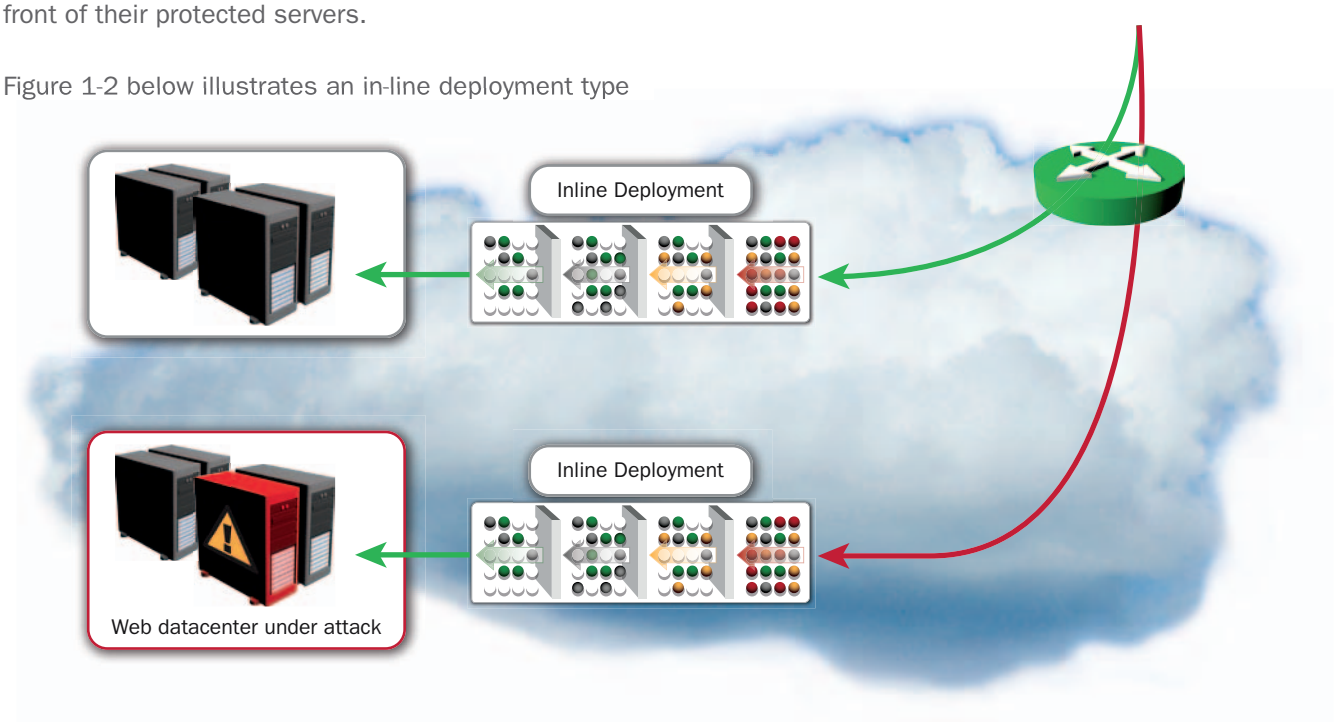

Figure 1-2: above illustrates an in-line deployment type

This approach holds several benefits for online companies. The most outstanding is its capability to provide immediate detection and response to attacks. Another clear benefit is the capability to detect and prevent attack beyond high volume DoS, such as network and application pre-attack probes, “low & slow” DoS attacks, network intrusions, malware propagation, and more (some organizations will choose both out-of-path and in-line deployment types in order to get full protection benefits for their servers).

Radware Attack Mitigation Solution (AMS)

Radware’s attack mitigation solution incorporates cutting edge behavioral analysis technologies coupled with dedicated high performance hardware to confront all types of DDoS attacks.

The solution was designed to work as an in-line (“always on”) solution, as well as an out-of-path scrubbing center. The solution is comprised of multiple DoS & DDoS layers of defense, including network-based protections and application layer protections which also cover SSL based DoS & DDoS attacks. The solution consists of two Radware products that work in sync in order to mitigate both clear and encrypted DoS attacks:

- **DefensePro**
  Radware’s DefensePro is an advanced attack mitigator with dedicated high performance hardware to confront all types of DDoS attacks. DefensePro’s layers of defense contain security technologies that were designed to detect and mitigate both high rate DoS & DDoS and low & slow attacks in the network and application layers, traffic anomaly attacks, connection-based misuse attacks, service cracking attacks, and application scan pre-attack probes – all of which misuse network and application resources and are part of multi-vulnerability based attack campaigns.

- **Alteon**
  Radware's application delivery product provides advanced application acceleration capabilities including a powerful SSL acceleration engine. The Alteon product provides the extendable throughput that large online businesses need.

Figure 2-1 below zooms in on a scrubbing center that includes Radware's mitigation equipment[1]:

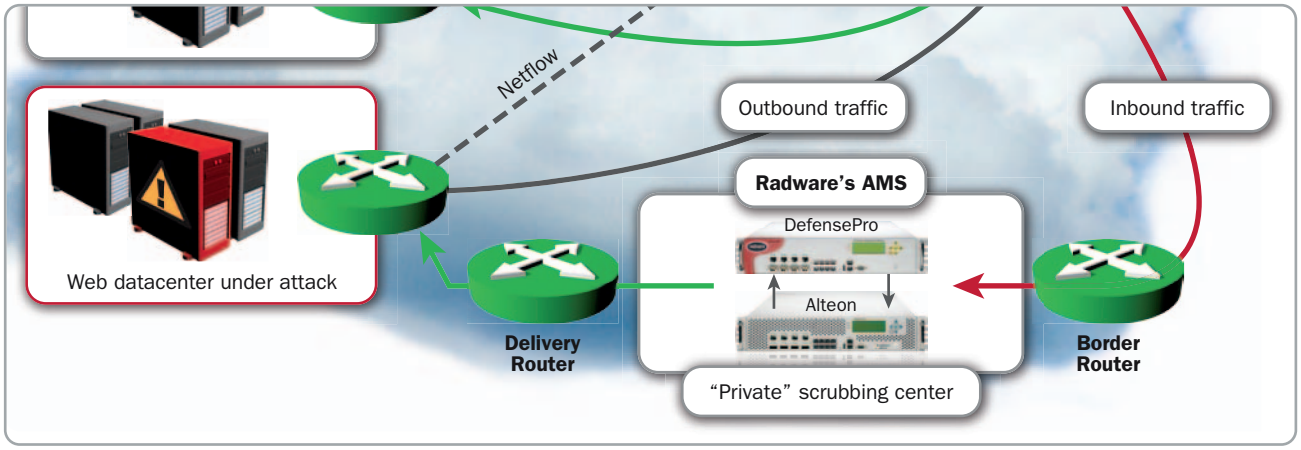

Figure 2-1: Radware's Attack Mitigation Solution (AMS)

Typical to this deployment type, once a DoS attack is identified, traffic is diverted to the scrubbing center. DoS attacks are immediately mitigated from the clear traffic portion by the DefensePro product. The encrypted traffic portion is automatically diverted to Alteon's SSL acceleration engine, decrypted, and sent back to the DefenensePro for further mitigation actions. More detail about the SSL termination process will be provided in the following sections.

Figure 2-2 below describes the main layers of defense that the attack mitigation solution includes:

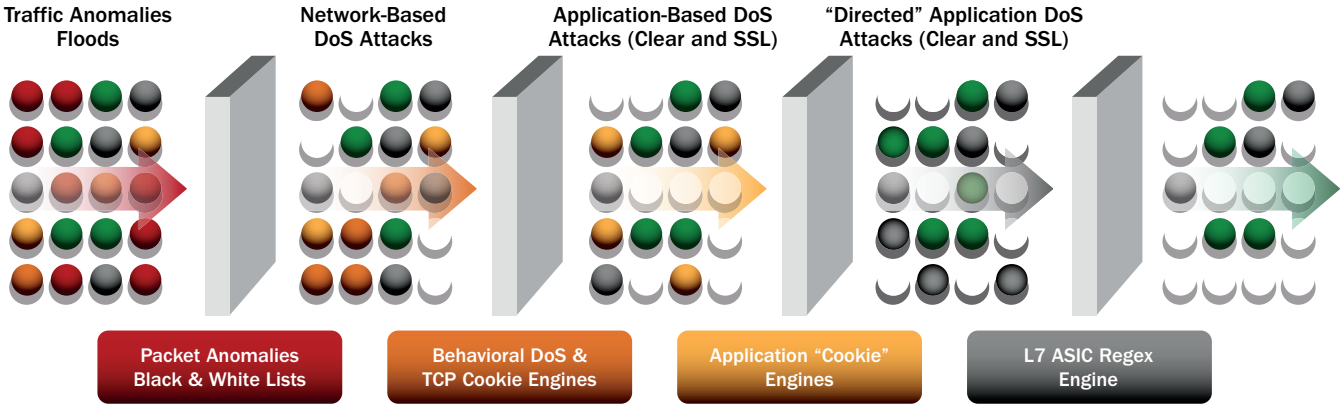

Figure 2-2: AMS Layers of Defense

All of the above DoS layers of defense were designed to meet the scrubbing center's strict requirements, as specified earlier in this paper.

[1] Same solution can be deployed in an in-line approach as well

Traffic Anomalies and Network-based DoS Layers of Defense

These two layers of defense were designed to detect and mitigate high volume network-based DDoS attacks. They cover all types of L3 and L4 DoS threats. The main ones include:

- Packet anomaly attacks
- IP Fragment floods
- TCP, UDP, ICMP, IGMP packet floods
- TCP spoofed SYN Attacks
- TCP connection flood attacks
- Known DoS attack tools

Detection and mitigation of these threats is undertaken by multiple security technologies, including behavioral based analysis, RT signature generation, TCP cookie mechanisms, rate limit engines, black lists, and others. For more details information about the security module, refer to Radware's security webpages.

The uniqueness of these two layers lies within the following main capabilities:

- The ability to differentiate between flash crowds and real DDoS attacks in any network environment
- Dedicated, powerful hardware for network DoS mitigation

These two unique capabilities allow the system to be more accurate in both detection and prevention of DDoS attacks, and block higher rate of DoS attacks as compared to other solutions on the market.

Application-based DoS/DDoS Protections

This layer of defense is designed to detect and mitigate application-based DoS attacks. This is done mainly by an advanced application challenge-response technology.

It covers L7 types of DoS threats.The main ones include:

- Get floods
- Post floods
- Bot-originated HTTP DDoS attacks
- SSL-based floods
- DNS-based floods

This layer detects attacks that don't necessarily misuse network and bandwidth resources, but rather more complex DoS & DDoS attacks that misuse application resources.

The uniqueness of this layer lies within the following main capabilities:

- Ability to differentiate between flash crowd and real application layer DDoS attacks, blocking the attack very accurately through different challenge/response technologies.
- Challenge/response engine that allows mitigating SSL based application floods.

Directed Application DoS/DDoS Attacks Protection

This layer of defense was designed specifically to repel DoS and DDoS attacks that require "special" filtering criteria. Some very advanced DoS and DDoS attacks cannot be mitigated well by generic mitigation methods (e.g., SYN cookies, application challenge/response, behavioral-based and rate limit-based mechanisms).

Two notable examples of these directed DoS attack techniques include:

- **"Slowloris"**
  One of the attack vectors in the WikiLeaks attacks campaign (Dec 2010), included this directed application level DoS attack. It is a piece of software which allows a single machine to take down another machine's web server with minimal bandwidth,
- **"Circle cache-control"**
  The recent Korean DDoS attacks in March 2011 included an HTTP DoS attack called "Circle cache-control." This type of application -evel DoS attack prevents the target server from using its caching mechanism and thus amplifies its impact.
- Attack tools like R.U.D.Y , Socketstress and their variants, are all part of this family of DoS threats.

This layer of defense is supported by a dedicated L7 Regex hardware component which allows flexible L7 filter definitions that search for specific content patterns anywhere in the transactions. This capability allows security managers and emergency response teams to analyze ongoing attacks that couldn't be defended by other protections, and to define "ad-hoc" protections against them. The uniqueness of this is based in the L7 Regex engine, supported by an ASIC based hardware that allows high performance detection and mitigation, as required for repelling DoS and DDoS attacks in multi-Gbps network environments, and the capability to also inspect encrypted (SSL) HTTP traffic.

SSL Attack Mitigation Flow

In order for the last two application layers of defense to identify and block encrypted HTTP DoS attacks, the mitigation solution requires that besides the DefensePro product, Alteon will also take an active part in the attack mitigation solution. The joint solution that Radware has designed is described in the following diagram, which includes the general traffic flow with the protection layers actions.

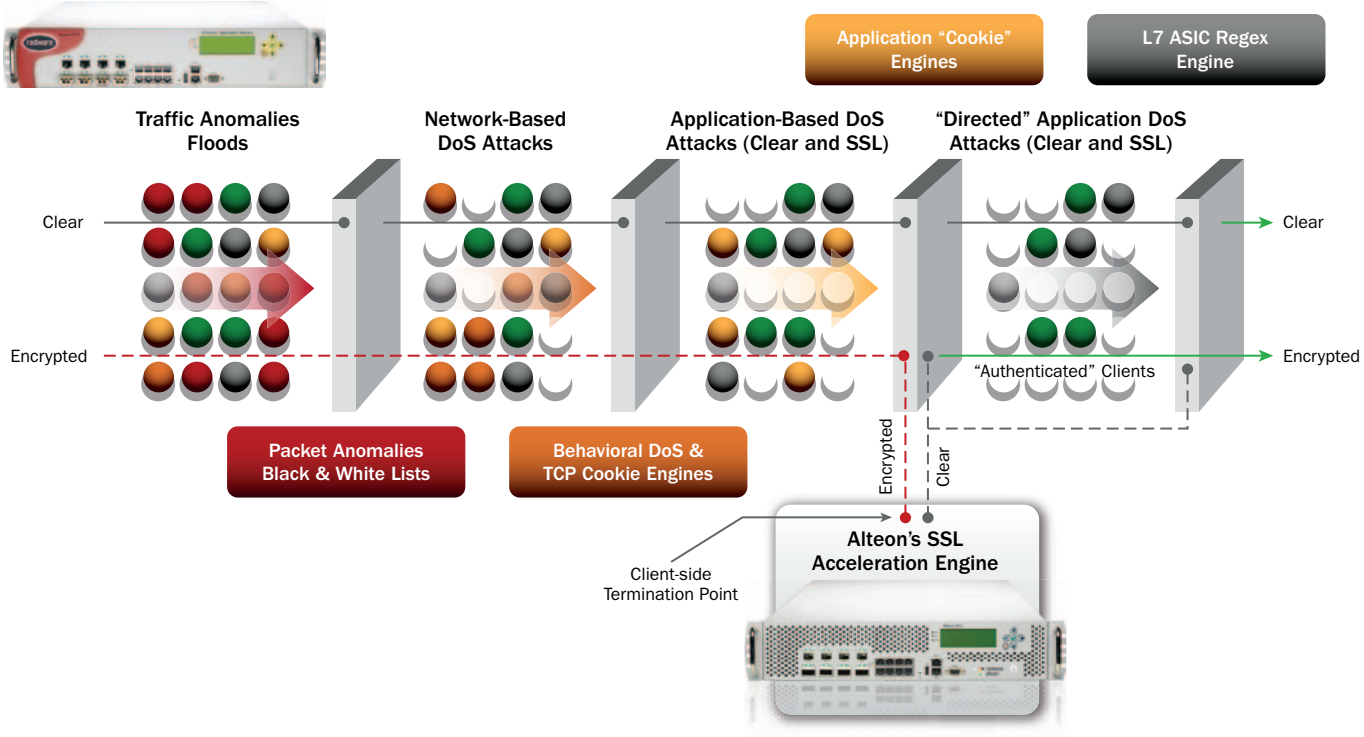

Figure 3-1: SSL Attack Mitigation Solution Flow

General Flow Description

Figure 3-1 above illustrates the following process:

- The DefensePro's layers of defense monitor both clear and SSL traffic.
- Network based (L3 and L4) anomalies and flood attacks are mitigated by the first two network security layers.
- Clear application-level DoS attacks are mitigated by the third and fourth application layers of defense.
- Encrypted (SSL) traffic is redirected to Alteon's SSL acceleration engine.
- The SSL engine terminates[2] the client connection, performs the SSL handshake, decrypts the traffic, and returns it to the application layers of defense in a clear text (marked as dashed blue lines).
- The two application layers of defense act as a "virtual protected server" and perform the following security actions:
  - Generate a client web challenge in order to validate that the client is a real one and not a Bot (both 302 redirect and JavaScript challenge actions are supported). The generated challenge action is encrypted by the SSL engine and returned to the client. In case the client is "authenticated" (i.e., responds correctly to the challenge), then the system forces the user to open a new SSL connection directly with the real protected server
  - The L7 ASIC Regex engine inspects the first client HTTP request and blocks it in case a pre-defined attack signature (database attack signature or custom one) is matched

For more details information about the layers of defense, refer to the *Rethinking Perimeter Security* white paper.

Mitigation Performance

Each security action specified above is supported by dedicated hardware that enables the repelling of high volume network and application DoS attacks. Three hardware components of the attack mitigation solution are responsible for this:

- **DME** – Denial of service mitigation engine that was designed to mitigate up to 12 M PPS SYN attacks.
- **SME** – L7 Regex ASIC (String Match Engine) that was designed to filter out the "directed HTTP DoS Attacks" through HTTP filters rules in a multi–gig traffic environment.
- **SSL Acceleration Engine** – A dedicated SSL acceleration ASIC that was designed to terminate SSL connections in very high rates.

Summary

Attackers are getting more sophisticated by the day, and specifically regarding online businesses, they have started to use SSL based DDOS attacks. They bypass standard DDoS protection countermeasures, and disembark directly at the online businesses application servers.

Standard DDoS mitigation solutions, whether in-line (perimeter), or out-of-path (scrubbing centers), currently do not offer any solution to fight the DDoS over SSL threat.

Radware AMS is the best-performing, and only solution, that offers online businesses full protection of their IT infrastructure against SSL based attacks, with a perfect match into any network deployment type, while maintaining excellent user response time even when under attack.

[2] The SSL termination requires that certificate will be installed on the SSL engine.