Table of Contents

Attack Mitigation Layers of Defense ............................................................................................................ 3
  Network-Based DDoS Protections .................................................................................................................. 3
  Application Based DoS/DDoS Protection ..................................................................................................... 3
  Network Scanning Protection ....................................................................................................................... 4
  Directed Application DoS/DDoS Attacks Protection .................................................................................. 4
Mitigation through Dedicated Hardware Architecture ..................................................................................... 5
  DME and Network Based DDoS Protection Layer ....................................................................................... 5
  L7 Regex Engine and the Directed Application DoS/DDoS Attack Protection Layer ................................. 5
  Multi-Purpose CPU’s - Other Layers of Defense ......................................................................................... 5
  Hardware Architecture That Was Tailored for Attack Mitigation .............................................................. 5
Radware’s Local Out of Path Mitigation Solution .......................................................................................... 6
  In-line Versus Out-of-Path Approaches ....................................................................................................... 6
  Radware’s Local-Out-of-Path (LOOP) Attack Mitigation Solution ............................................................. 7
  Radware’s LOOP Attack Mitigation Solution Summary .............................................................................. 8
Summary .................................................................................................................................................. 12
Attack Mitigation Layers of Defense
Radware’s DefensePro is an advanced attack mitigator incorporating cutting edge adaptive behavioral analysis technologies coupled 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 “low & slow” and high rate DDoS attacks in the network and application layers, service cracking, application scans—all of which misuse network and application resources.

Radware’s DefensePro includes the following layers of defense:

Network-Based DDoS Protections
This layer of defense is designed to detect and mitigate high volume network-based DDoS attacks through an adaptive network behavior-based engine. It covers all types of L3 and L4 floods. The uniqueness of this layer lies within the following main capabilities:

1. Ability to differentiate between flash crowds and real DDoS attacks in any network environment
2. Attack mitigation via a real-time behavioral signature that the system creates on the fly

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

Other traditional attack mitigation systems that are using rate-based technology are incapable of differentiating between legitimate and illegitimate traffic and are prone to blocking legitimate traffic while under attack or under a high load of traffic.

Application Based DoS/DDoS Protection
This layer of defense is designed to detect and mitigate bot originated application based DDoS attacks. This is done mainly through an application based behavioral analysis mechanism that learns and analyzes application level parameters such as HTTP request methods, reply types, transactions rates, and average object size. This layer detects attacks that don’t necessarily misuse the network and bandwidth resources, but rather more complex DoS & DDoS attacks that misuse application resources.

In addition to DoS/DDoS attacks, this layer also provides protection against application cracking attacks and application scanning, both of which are part of an information gathering process that cannot be detected effectively by traditional IPS signature based approaches.
The uniqueness of this layer lies within the following main capabilities:

1. Detection of abnormal repetitive patterns of application transactions, enabling it to differentiate between legitimate and bot originated transactions, thus blocking attacks very accurately
2. Ability to differentiate between flash crowd and real application layer DDoS attacks – an even more challenging task than for network based floods

These two unique capabilities allow the system to be more sensitive to application DDoS and misuse of applications resources, while at the same time maintaining a high level of mitigation accuracy.

Network Scanning Protection
This layer of defense is designed to trace the source of abnormal behavioral, such as any type of network scanning (“pre-attack” probes), sources that are infected with malware which propagates itself using network scanning activities. This layer analyzes, per source IP address, traffic parameters such as the number of new connections, port and IP address distribution and more in order to reach a conclusion about the source. Once it detects a source that generates scanning activities, it finds a behavioral pattern and accordingly creates a real-time signature which is used to mitigate the scanning activities.

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

1. The ability to detect high rate (scanning that misuse network resources) as well as stealthy low rate scans with virtually zero false positives
2. A very accurate behavioral analysis system that can block scanning activities while allowing legitimate traffic to go through, even from the same source of the attack

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.

A few examples of these attacks include the Mydoom.EA DDoS that took place in 2009 and took down on-line and government websites in the U.S. and Korea, even though they were all equipped with anti-DDoS solutions, as well as other “low-rate” DoS attacks such the “Slowloris” attack that took down Web servers all around the world.

Radware DefensePro’s last layer of defense is the String Match Engine (SME), a L7 Regex engine which allows flexible L7 filters definitions that search for specific content patterns anywhere in the transactions. This capability allows security managers to analyze ongoing attacks that couldn’t be defended by other protections, and define “ad-hoc” protections against it.

The uniqueness of this 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.
Mitigation through Dedicated Hardware Architecture
Each layer of defense in the DefensePro is supported by hardware architecture that was designed to maximize the performance of protection.

DME and Network Based DDoS Protection Layer
This layer is supported by a DoS Mitigation Engine (DME). The DME is a dedicated network processor that was optimized to perform L3 and L4 filtering operation at a rate of over 10 Million PPS.

String Match Engine (SME) - L7 Regex Engine and the Directed Application DoS/DDoS Attack Protection Layer
This layer is supported by a a String Match Engine (SME), a L7 Regex acceleration engine. The engine is an ASIC based hardware component that was optimized to perform application pattern matching in multi-Gbps network environments.

Multi-Purpose CPU’s - Other Layers of Defense
The other protection layers and network based operations are done by multi-purpose CPUs which provide the required flexibility and scalability for the more standard operations, such as stateful and statistical analysis which are part of the behavioral analysis modules.

Hardware Architecture That Was Tailored for Attack Mitigation
The main advantage of DefensePro’s hardware architecture rests in its ability to completely separate the mitigation tasks, each one in a different dedicated hardware component, thus preventing internal resource cannibalization that typifies other attack mitigation products.

Repelling the multi-million PPS L3-4 DDoS attack is done solely by the DME hardware component while attacks that need to be mitigated through DPI (Deep Packet Inspection) utilize the L7 Regex acceleration ASIC. At the same time, legitimate traffic that should continue to be processed by the stateful analysis modules and t feed the statistical analysis modules in the system is being processed by the multi-purpose (multi-cores) CPU’s.

This hardware architecture provides higher and more predictable performance figures than other attack mitigation systems.
Radware’s Local Out of Path Mitigation Solution

In-line Versus Out-of-Path Approaches

Attack mitigation devices typically select one of two deployment approaches, in-line and out-of-path. Each one has its own advantages and disadvantages.

The out-of-path approach – this approach usually uses “scrubbing centers” which are responsible for the mitigation part and see traffic only during the attack time. Detection is done by an out-of-path detection system which is mainly based on NetFlow statistics. Once an attack is detected, the relevant traffic is diverted to the scrubbing center (routing is changed through a BGP announcement), attacks are mitigated, and then sent back to the protected entity. In this approach, the scrubbing center usually sees only ingress traffic i.e., response traffic is routed in the original path.

The in-line approach – detection and mitigation is usually done by the same device that is deployed in-line and sees traffic all the time (in peace and attack times). The in-line device is usually a transparent one, i.e., doesn’t have an IP address, and inspects all traffic, both inbound and outbound in both network and application layers. Once an attack is detected, the same device will immediately try to block it.

The main pros and cons of each approach are listed below:

**In-line vs. out-of-path (In-line advantages)**

- **Higher security coverage** - the inline approach provides full visibility into the traffic from L2 and up to L7. Thus, the achieved security coverage can be very high. The out-of-path approach is based mainly on NetFlow statistics, and can therefore only analyze traffic based on L4 parameters, which limits its security coverage to network-based attacks only.

- **Detection response time** – with the in-line approach, detection can be done in real-time since all traffic can be processed by the attack mitigation device online. In the out-of-path approach the detection is limited by the router NetFlow statistic cycles which can take minutes to go from one cycle to another.

- **Mitigation response time** – with the in-line approach, mitigation response is very fast as there is no need for any routing changes – the same security devices apply the blocking rules immediately. In the out-of-path approach mitigation is dependent on the time it takes to divert traffic through the scrubbing center and the time it takes for the mitigation device (which didn’t see the traffic yet) to apply the correct filters.

- **Mitigation in a symmetric traffic environment** – Attack mitigation in an ingress only environment such as is offered by a typical out-path scrubbing solution is limited. Some DoS and DDoS attacks require the security device to “see” both traffic directions in order to mitigate the attack accurately (e.g., application attacks that violate the stateful rules and others).

- **Deployment & BGP Disruption** - The In-line deployment approach doesn’t require re-configuration of network elements and there is no need for dynamic routes (e.g., BGP announcements) The out-of-path architecture mandates the security manager to apply dynamic routing rules through BGP. This approach can be risky as it is more prone to mistakes that can lead to network disruptions with high impact e.g., a wrong diversion instruction can lead to unnecessary latency or loss of connectivity.

**Out-of-path vs. Inline (out-of-path advantages)**

- **Point-of-failure** – In-line deployment adds an additional network point of failure while the out-of-path approach becomes one only during attack times and only for the attacked target.

- **Latency** – In-line deployment can potentially increase network latency while the out-of-path approach can increase it only during attack times and only for traffic that is associated with the attacked target.

- **Detection scalability** – The out-of-path approach is based on NetFlow statistics that are collected from the existing network infrastructure (routers and switches). This makes the detection system a very scalable one. It means that the detection performance capabilities are limited to the performance of the existing routers.
and that detection can cover, from one location, any part of the network that provides NetFlow statistics. The In-line approach will see only the local traffic and detection performance capabilities are limited to those of the security device.

**Radware’s Local-Out-of-Path (LOOP) Attack Mitigation Solution**
In order to benefit from both in-line and out-of-path approaches, Radware’s DefensePro provides a local out-of-path solution.

The local out-of-path provides the same advantages that the in-line approach provides, while eliminating some of the weaknesses of the same approach.

**The LOOP Solution**
The local out-of-path capability allows Radware’s DefensePro to work in a tap-like mode, as long as no attack is detected. Upon attack detection, a powerful smart switch routes the relevant traffic through the chain of protections for mitigation purposes. From a network operations point of view, this would allow easy integration into any network critical path.

The main idea is to perform in-line traffic processing only for networks or specific IP addresses and even applications that are currently under attack while the detection technology benefits from the same degree of accuracy as the in-line approach as traffic is mirrored to flow through DefensePro and goes through the same logic.

**How Does it Work?**
In peace time, traffic is copied to the protected system. Upon attack detection, a smart bypass switch diverts only the traffic that is destined to the attacked target through the protection system. Clean traffic is then sent back to the protected network. Granularity of redirection can be done per destination network (range or network mask, individual IP addresses and L4 port numbers).

The following figures illustrate the LOOP operation in peace and in attack times:

**Figure 3 – LOOP in peace time**

![Image of LOOP in peace time](image-url)
The out of path solution mandates that the mitigator device not be in-line during peace time operations. The LOOP bypass switch installed in the traffic path of a protected segment presents a robust way to introduce the appliance into the network, and provides immediate mitigation capabilities when required. In normal operation, this mode provides a native ability for DefensePro to baseline traffic patterns and alert on occurring attacks without any limitation.

During attacks, the LOOP switch is reconfigured to change the traffic flow direction as per Figure 4. The redirect command can be engaged either manually or automatically, at which point attack traffic processed through the DefensePro is cleaned from attacks.

**Radware’s LOOP Attack Mitigation Solution Summary**

The local out-of-path solution eliminates some of the limitations that typify the in-line deployment approach, while maintaining all of its security advantages:

- **Point of failure** – the robust high capacity LOOP switch removes the point-of-failure issue
- **Latency** – the LOOP switch is a dedicated hardware with virtually zero latency
- **In-line advantages** – all advantages as described in the previous section including security coverage, detection response and mitigation response are maintained

The final result is a system that benefits from the two approaches, in-line and out-of-path. Network operation concerns such as adding point of failure and increased latency are solved by the LOOP solution while the security coverage concerns are addressed by all layers of protection as described in the previous sections of this paper.
**Competition Analysis**

This section summarizes the advantages of the DefensePro Attack Mitigation device as compared to other existing solutions in the market today.

**Security Coverage – Radware’s “LOOP” Solution Versus Out-of-Path**

Figure 5 above describes the advantages of the DefensePro Attack mitigation solution when comparing it to the typical out-of-path, NetFlow based, attack detection solution.

Both detection coverage and detection sensitivity are higher as a result of the full visibility into the network traffic from L2 and up to L7.

**Summary**

Radware’s DP attack mitigation product presents a solution that takes advantage of both deployment approaches: the in-line and out-of-path. The hardware architecture was designed to block both high rate network DDoS attacks as well as attacks which require DPI capabilities.

Performance is high and predictable, as a result of the unique hardware architecture that utilizes dedicated hardware for each attack type, including isolated hardware components that repel large scale L3-4 DDoS attacks, dedicated DPI ASIC for application directed DoS attacks and multi-purpose CPU’s cores for other operations.

Radware’s patented behavioral analysis algorithms utilized by DefensePro allow automatic mitigation of attacks with a minimum of human intervention while maintaining a high level of accuracy, even against the low rate (stealthy) attacks.

The local out-of-path solution is designed to avoid network operation concerns that are usually raised when a security device needs to be integrated, in-line, into a critical network path. Network operation concerns such as latency and additional point of failure are solved by Radware’s LOOP attack mitigation solution.

For more information, refer to Radware’s website [www.radware.com](http://www.radware.com)

© 2010 Radware, Ltd. All Rights Reserved. Radware and all other Radware product and service names are registered trademarks of Radware in the U.S. and other countries. All other trademarks and names are the property of their respective owners.