SOFTEL
enabling networks

Radware DDoS Solution Deployment

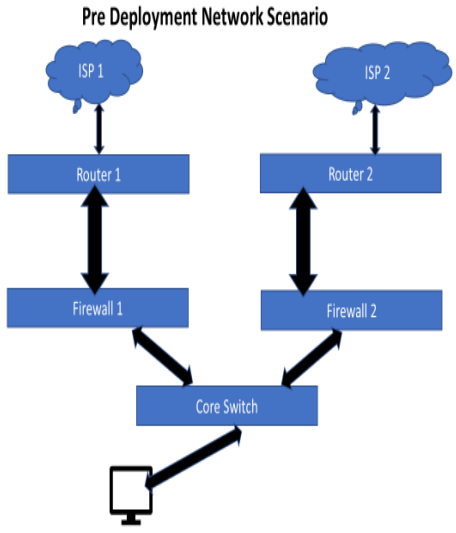
One of our client we have implemented DDoS solutions in their Data Center and Disaster Recovery Sites. They had the requirement to prevent their infrastructure from cyberattack that tries to make their website or network resources unavailable.

.

SCOPE

Distributed denial-of-service (DDoS) attacks are increasing in frequency and ferocity. Powerful IoT-botnets for hire over the darkweb make launching large-scale attacks accessible, effortless and cheap. Professional hackers are continuously seeking new ways to disrupt the flow of network traffic and undermine the user experience, resulting in loss of revenue, tarnishing of the brand and increased customer churn rates.

Real-time perimeter attack mitigation device secures organizations against emerging network multivector attacks, powerful DDoS campaigns, IoT botnets, application vulnerability exploitation, malware and other types of cyberattacks. DefensePro's proven behavioral-based technology is designed to prevail over modern sophisticated attack tools and cybercriminals.

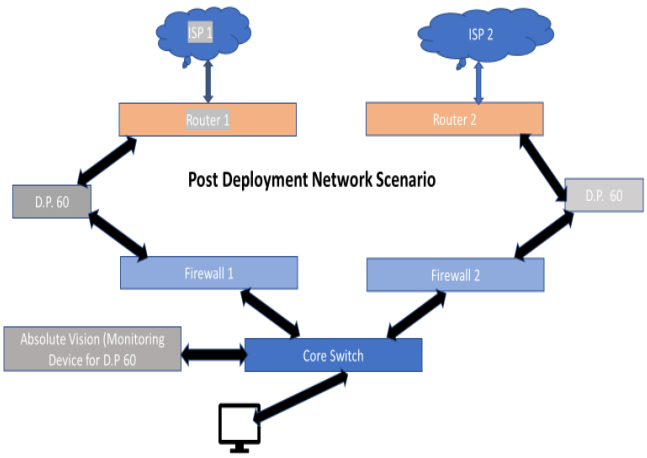


THE CHALLENGES

- DDoS stands for Distributed Denial of Service. DDoS is a type of cyberattack that tries to make a website or network resource unavailable. An attacker coordinates the use of hundreds or thousands of devices across the internet to send an overwhelming amount of unwanted to the target, which could be a company's website or network

- Almost any type of internet-facing connected device could be a potential DDoS resource: Internet of Things (IoT) devices, smartphones, personal computers, and powerful servers.

- Packets of data are used to communicate on the internet. A DDoS sends unwanted packets, which can be very large packets with lots of data, small packets very rapidly, or packets that require extra processing. It can also make the targeted device waste time waiting for a response that never comes. The target is kept so busy dealing with malicious packets and improper communication methods that there is little, or no time left to respond to normal incoming requests – so legitimate users are denied service.



Benefits of Defense-Pro

- **Dedicated Hardware to Fight Attacks**

  Defense-Pro uses a dedicated hardware platform to prevent high volume DoS attacks and DDoS flood attacks without impacting legitimate traffic.

- **Automated Zero-Day DD0s Attack Protection**

  With a patent-protected real-time signature creation technology, Defense-Pro is a DDoS defense device that can automatically generate DDoS prevention and protection for zero-day and unknown attacks. Within 18 seconds, Defense-Pro can detect, characterize, and generate an optimal signature to block unknown attacks with a minimal false-positive rate.

- **Behavioral-Based Detection for Highest Accuracy**

  Based on Radware's patented behavioral-based detection technology, Defense-Pro, can accurately detect attacks in a very short timeframe with minimal false positives.

- **Smart SSL Attack Mitigation**

  Patent-protected SSL attack mitigation solution that protects from all types of encrypted attacks with reduced-latency solution. Supports asymmetric deployment environments which are crucial in cloud-based deployments such as scrubbing centers, service provides, and multi-homed deployments.

- **High Mitigation Capacity to Support Large Scale Organizations**

  Up to 300Gbps of mitigation capacity and 230M PPS while allowing customers to enjoy the widest range of simultaneous cyber-attack protection in the industry. Multi-tenant support for a growing number of customers with increased complexity and capacity.

- **Fully Managed Piece of Mind**

  On-premise device management provided by Radware's Emergency Response Team (ERT) includes security experts that setup, manage and tune the device to keep it synchronized with business processes and policies.

- **Accuracy of Inline and Scalability of Out-of-Path**

  Defense-Pro DDoS protection and DDoS prevention devices can be deployed inline or out-of-path (OOP) in a scrubbing center to provide the highest mitigation accuracy within the shortest time.

- **Single point of contact**

  ERT fights the attack during the entire campaign, no other vendors involved

- **Flexible Payment Models**

  Available as a fully managed service with flexible payment models (CAPEX or OPEX based subscription)

- **Attack Vectors**

  Over 100 attack vectors on the network and application layers are detected and mitigated including

  Large volume network attacks

  SYN floods

  Low and slow

  HTTP floods

  SSL encryption

  Brute force

  BGP table attacks

  Session attacks

  Invasive scans

Conclusion

Radware offers a complete line of DDoS mitigation solutions, advanced technologies, and value-adding features to meet the full range of enterprise and service provider DDoS mitigation requirements. Radware also offers DDoS mitigation solutions tailored to meet the specific needs that are most pressing in various industries. Moreover, Radware continues to identify new and emerging attack trends in order to provide the highest levels of protection against increasingly sophisticated and dedicated DDoS threat actors. With its strong overall performance,