radware

Smart Network. Smart Business.

Protecting DNS Critical Infrastructure Solution Overview

Radware Attack Mitigation System (AMS) - Whitepaper

Table of Contents

Introduction

DNS is a critical infrastructure of the Internet as every web transaction involves a DNS service provided by the Internet service provider. A successful attack against DNS services that manages to disrupt these services will halt all other Internet-based services.

Although carriers and service providers provision various mitigation tools, the current DNS infrastructure is still vulnerable and is subject to an increasing variety of attacks that are becoming ever more sophisticated and difficult to mitigate. Therefore, securing DNS service requires rethinking on perimeter security with dedicated tools to identify and mitigate these new breed of attacks on DNS services.

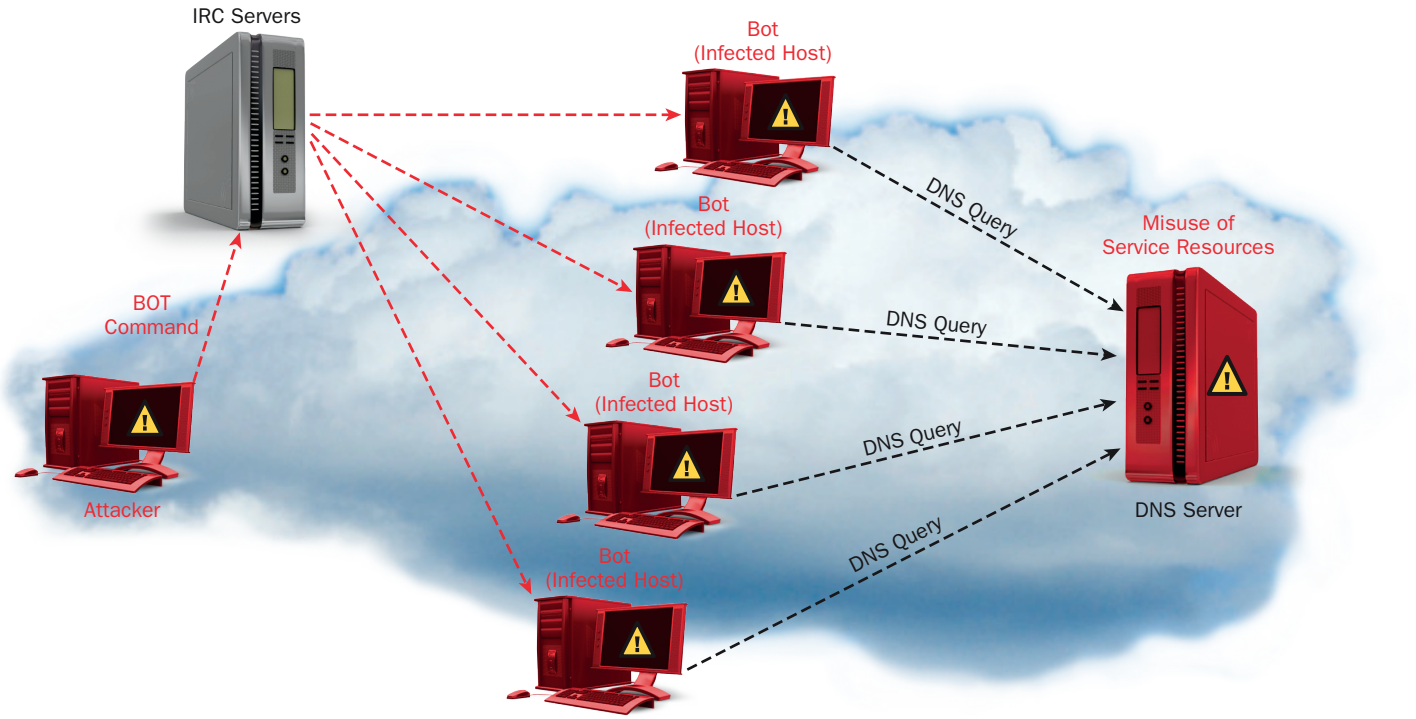
This paper outlines the recent DDoS attacks on DNS services and the challenges of mitigating those attacks. It presents Radware's DDoS DNS attack mitigation solution and its unique differentiators that make it the world best mitigation tool for DNS service attacks.

DNS DDoS Attacks are Growing and Evolving

DNS is a carrier and service provider critical to the infrastructure as every web transaction involves a DNS query for name-to-IP-address resolution prior to accessing the requested website. Degrading, or even shutting down the DNS service of a service provider, has an immediate impact on Internet-based services, and it can result in eliminating legitimate users from accessing the Internet. Attackers understand that service providers take security measurements to protect their DNS infrastructure and therefore, they generate more sophisticated attacks with increased impact on the service.

This section discusses the recent attack techniques deployed by attackers aiming to disrupt the DNS service:

- **DNS Flood Attack** - Utilizing multiple sources of compromised computers, called Botnets, the attacker generates a distributed, volumetric denial of service attack that floods the DNS servers. Since DNS service is typically carried over UDP, it is more vulnerable to volumetric attacks. According to the DNS standard, the DNS servers process every request, which results in a DNS servers' overload. This behavior allows the attacker to successfully compromise DNS service, utilizing a surprisingly small amount of Botnets.



- **DNS Amplification Attack** - A standard DNS request is natively smaller than the DNS reply. In a DNS amplification attack, the attacker carefully selects a DNS query that results in a lengthy reply that is up to 80 times longer than the request. This results in an increased load on the DNS servers, compared to the "regular" DNS flood attacks.

- **DNS Recursive Attack** – This is an attack amplification method of DNS flood attacks, where the attacker generates a distributed, volumetric denial of service attack that floods the DNS servers. However, in this attack, the attacker turns on the recursive flag within the DNS query packet. When the recursive flag is turned on, it forces the DNS server to perform the name resolution itself, rather than redirecting the request to another server, and to reply to the sender with the resolution. In a DNS recursive attack, the attacker slightly changes the requested domain name in every DNS query so that the DNS server would not be able to reply with a cached result, forcing the server to lookup for the domain name multiple times. This results in a severe load on the DNS service, until it's not available for legitimate users.

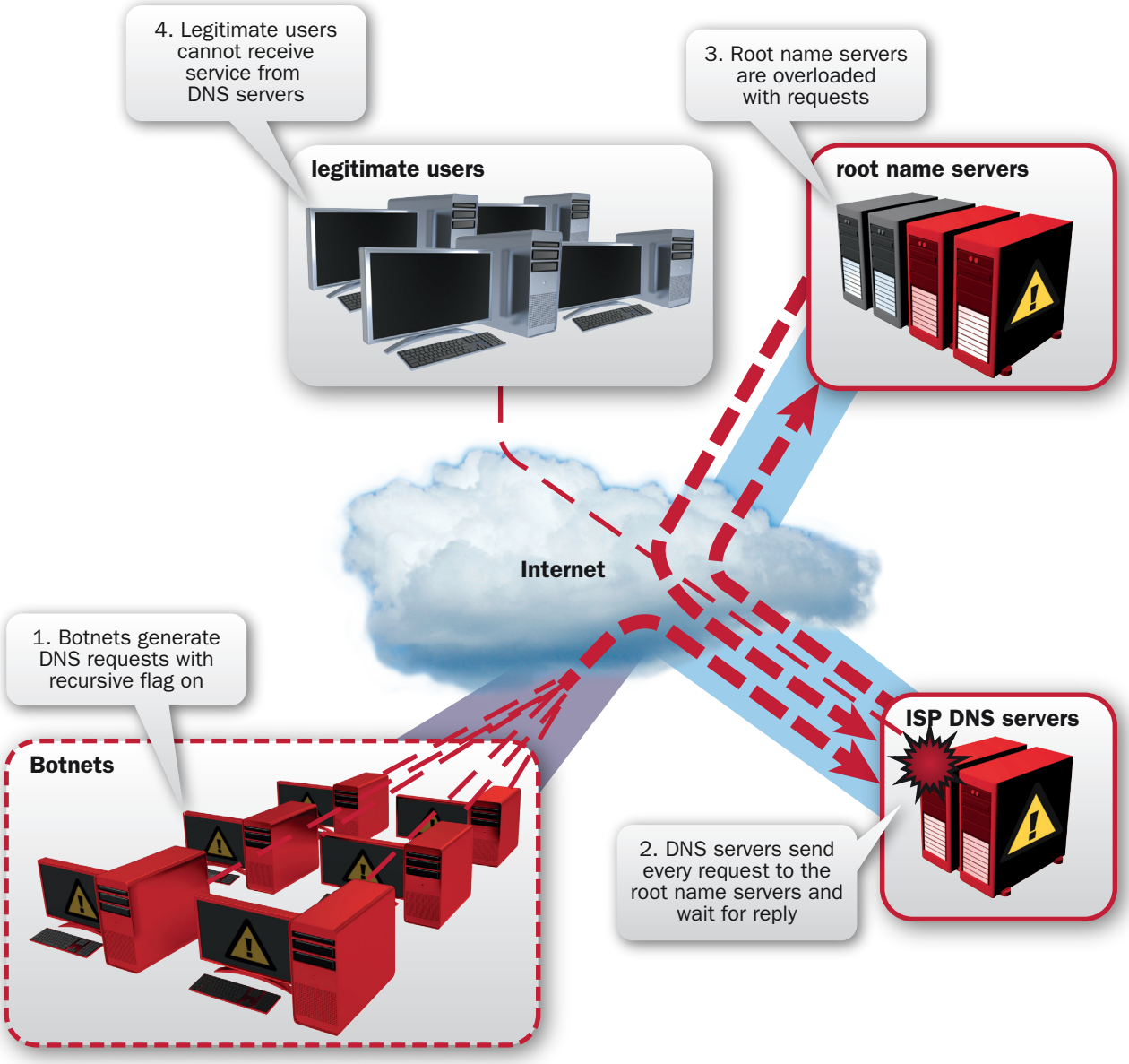


Diagram of DNS Recursive Attack

Challenges of Protecting DNS DDoS Attacks

As described above, DDoS attacks on DNS servers become more complicated to mitigate, and today's attack mitigation tools must be able to meet unique challenges in order to successfully block DNS attacks:

Mitigation tools must have deep knowledge of DNS traffic behavior – Sophisticated attackers take advantage of the DNS protocol behavior in order to generate more powerful attacks with greater potential to hurt the DNS service, such as the DNS recursive attack. To mitigate such attacks, every single field in the DNS protocol must be carefully analyzed, utilizing a deep knowledge of the DNS protocol, and solid understanding of DNS traffic behavior.

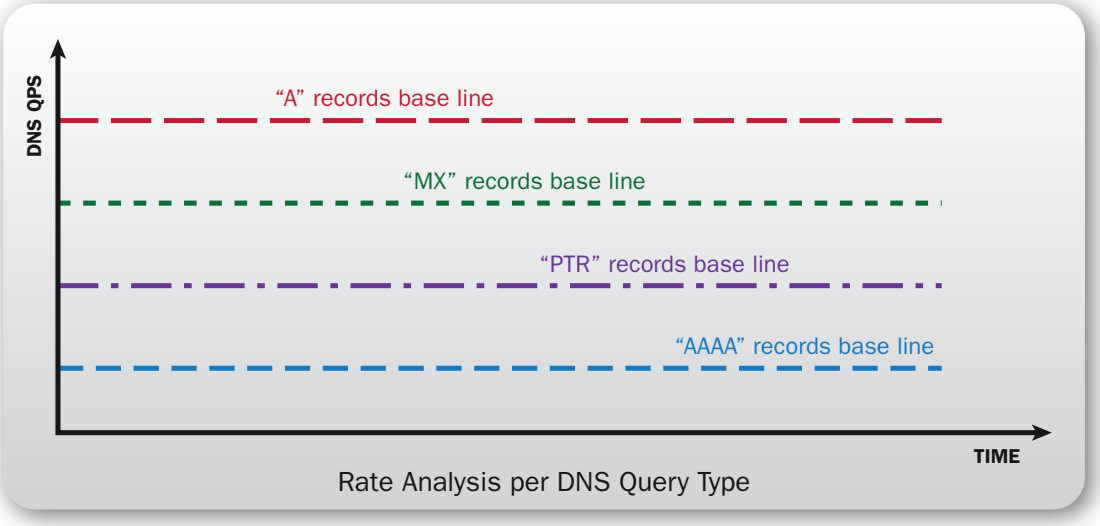
Mitigating high rate of DNS packets – DNS DDoS attacks involve a large volume and high rate of flood packets. The mitigation device must be able to process a high volume of traffic, usually several million packets per second,in order to block all attack packets, while still providing enough bandwidth to process legitimate DNS traffic.

Accurate Mitigation – Failure to distinguish between legitimate DNS traffic and attack DNS traffic results in false positives, for example, legitimate users who cannot access any Internet service. The impact of false positives on the Internet service provider is significant, including reputation degradation and loss of revenues. Therefore, today's mitigation tools must be accurate, and provide service to legitimate users even under attack.

Provide best quality of experience, even under attack – In addition to mitigation accuracy, the mitigation tools are required to continue and provide best quality of experience to legitimate users, even under attack. This requires a very low latency from the mitigation tools and the ability to provide a device that is based on hardware engines and accelerators, rather than a software-only based device.

Radware Solution for DNS DDoS Attacks

The Radware solution for DDoS DNS attacks is based on its DNS flood attacks protection feature, part of Radware's renowned Behavioral DoS module in its DefensePro product line. The DNS attack mitigation solution can be divided into three phases: the detection phase, creating a real-time signature phase, and the mitigation phase.

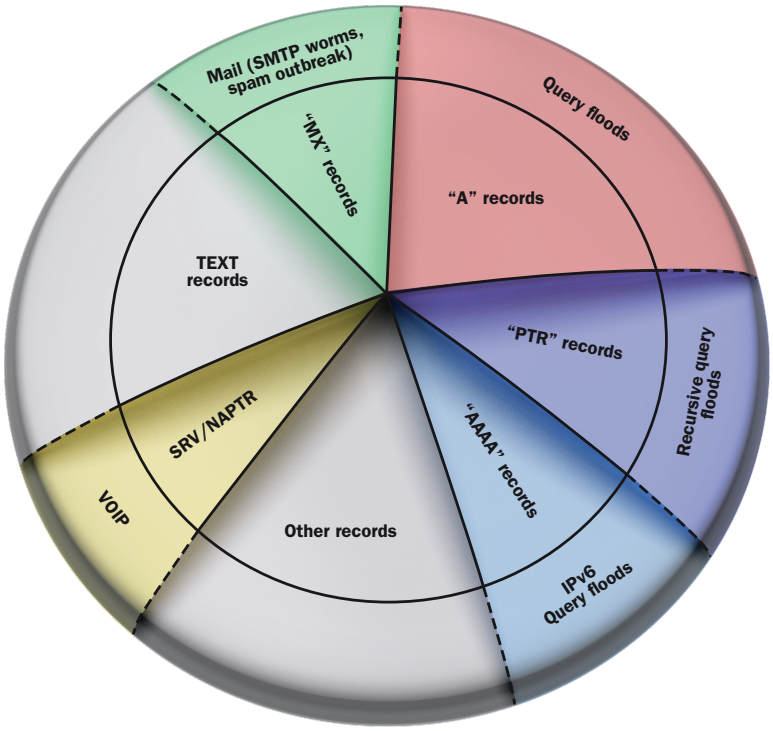


Rate analysis per DNS query type

Detection Phase

During the detection phase, DefensePro monitors all inbound DNS traffic on UDP port 53 and learns the baseline of normal DNS traffic behavior. For each DNS query, it updates the baselines per query type, query rate, and rate invariant as well as its relative share among all DNS queries.

The DNS attack mitigation continuously generates a degree-of-attack score, using a fuzzy-logic[1] engine. The fuzzy logic module is a multi-dimension decision engine that detects attacks in real-time, based on evaluation of real-time network data with current baselines. When the degree of attack score exceeds the value that is considered as an attack, the system moves to the mitigation phase.



DNS query distribution analysis

Creating Real-Time Signature

To successfully mitigate a DDoS DNS attack, DefensePro creates an automatic, real-time signature that blocks the DNS DDoS attack without any human interaction. Using samples of real-time traffic that deviates from the baseline traffic, DefensePro is looking for characteristic parameters of the ongoing anomaly in the suspicious traffic.

The following parameter types, as well as others, are analyzed by the automatic signature creation module:

- Packet checksums
- Packet size
- Packet Identification number
- TTL (Time to Live)
- Fragment offset
- Source IP address
- Destination IP address
- Ports numbers
- DNS Qname – domain name
- DNS Query ID – query identification number
- DNS Query count (Qcount)

Once the values of these parameters are flagged as "abnormal," the system creates a real-time signature based on the suspicious parameters, and it activates a signature optimization mechanism called the "closed-feedback loop."

The closed-feedback module is responsible for creating the narrowest, but still effective, signature-blocking rule. Each one of the suspicious flagged parameters can include multiple values, detected by the automatic signature generation mechanism. The closed-feedback module "knows" how to tailor these values through AND/OR logical relationships. The more AND logical relationships are constructed between different values and parameter types, the more accurate and narrow the blocking signature rule is considered to be. In order to create the logical relationship rules between the detected signature values, the closed-feedback module uses the following feedback cases:

- **Positive feedback:** The traffic anomaly was reduced as a result of the decided blocking signature rules created by the module, the system continues to use the same action and tailors more attack characteristic parameters (i.e., signature types and values), through as many AND logical relationships as possible.

[1] To read more on Radware's Fuzzy Logic engine, download: http://www.radware.com/Thank_you_download.aspx?ID=5557

- **Negative feedback:** This means that the degree of traffic anomaly was not changed, or was increased. The system stops using the last blocking signature rules and continues to search for more appropriate ones.

- **Attack stopped feedback:** If the attack stops, then the system will stop all countermeasures immediately (i.e., remove the signature rule).

The real-time signature is applied to suspicious traffic in the next phase.

Mitigation Phase

During the mitigation phase, DefensePro utilizes the real-time signature to detect suspicious sources of the DNS attack and it performs the following escalation steps to stop the attack:

Escalation #1: Signature based Challenge – DefensePro challenges DNS A and AAAA queries that match the real-time signature. The purpose of the challenge is to distinguish between legitimate traffic created by legitimate users, and DoS traffic generated by Botnets.

Escalation #2: Signature based Rate Limit – If after escalation #1, the closed feedback module still reports that the attacks continues, DefensePro performs another escalation, which is to limit the rate of DNS traffic that matches the real-time signature.

Escalation #3: Collective Challenge – The next escalation step is to challenge all DNS A and AAAA queries traffic, not only from the suspicious sources, but from all users. Again, the purpose of this challenge is to distinguish between legitimate traffic created by legitimate users and DoS traffic generated by Bbotnets.

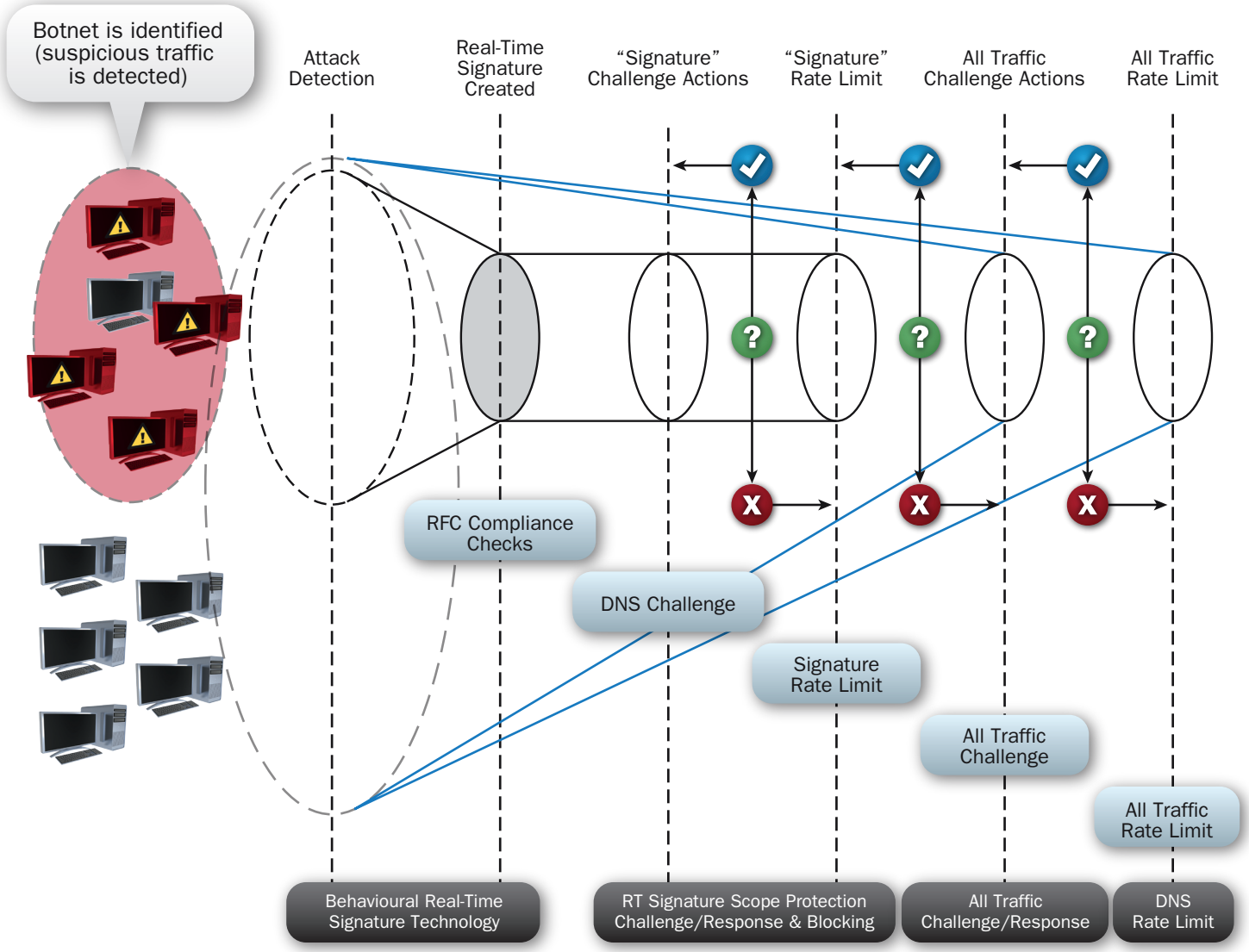
Escalation #4: Collective Rate Limit – If the attack continues, the last resort and the last escalation steps is to perform rate limit on all DNS traffic according to the defined maximal query rate.

DNS Challenge and the Selective Discard Mechanism

As described above, during the escalation steps, DefensePro challenges the DNS sources to verify that they are legitimate users rather than attackers. The challenge is activated on query types A and AAAA, and it is based on RFC definitions. During the challenge, DefensePro ignores the first packet that it receives from a DNS source. According to the DNS standard, a new DNS packet should be retransmitted within limited timeslot containing the same Qname. To issue challenges and to verify that the DNS source response to the challenges, DefensePro uses a statistical table and function, which is called the Selective Discard Mechanism (SDM). Each entry in the SDM table receives a score for each query reaching the table. When a source answers the challenge correctly, its score increases and then gets listed in the internal DNS authentication table. When a source fails to answer a challenge correctly, its score decreases.

To minimize the impact on user experience, while challenge operations are being conducted, the protection module uses an authentication table, which stores for a specified period, the source IP addresses that responded properly to the challenge.

To avoid misclassification of proxy devices, either as legitimate or as attacking entities, the SDM reduces source scores with each new query that reaches the module and is not challenged. When the score of a source falls below a certain score, it will be challenged again. A proper response to the challenge will raise the source's score and the next few queries from it will not be challenged.



Challenge/Response & Action Escalation System

Diagram: DefensePro 3 phases of DNS attack mitigation

DefensePro Meets the Challenges of DNS DDoS Mitigation Tools

As described above, there are several very unique challenges that DNS DDoS mitigation tools must meet in order to efficiently and successfully block attacks. DefensePro is the industry-first DNS DDoS mitigation device that meets all these unique challenges:

Mitigation tools must have deep knowledge of DNS traffic behavior – DefensePro understands DNS traffic and learns it normal behavior continually, so it immediately identifies abnormal DNS traffic. Moreover, DefensePro analyzes every field in DNS traffic to identify abnormal packets and to create its real-time signatures with high accuracy.

Mitigating high rate of DNS packets – Utilizing its DoS Mitigation Engine (DME), a network processor-based hardware accelerator, DefensePro can challenge 2M DNS queries per second and to process up to 12 million packets per second of attack traffic. The attack traffic does not affect DefensePro capabilities to handle legitimate traffic and it can handle multi-gigabits of legitimate throughput traffic under attack.

Mitigation accuracy – With unique DNS challenges and accurate analyzing of DNS traffic behavior, DefensePro provides a very accurate distinction between legitimate DNS traffic and attack DNS traffic results, with minimal false positives. This enables the service provider to continue to serve its legitimate users, even under severe attack.

Provide best quality of experience, even under attack – DefensePro has a unique architecture that is based on several hardware engines and accelerators that guarantee a minimum latency to all processed traffic, and especially to the legitimate traffic. The DNS challenges that are described above are applied by the real-time signature only to suspected sources of attack traffic. This guarantees a best quality of experience to legitimate Internet users, even under attack.

Summary - The World's Best Mitigation Tool for DNS DDoS Attacks

DefensePro is the world's best mitigation tool for DNS DDoS attacks, as it provides a unique set of patented tools and challenges to successfully mitigate sophisticated, yet volumetric, DNS DDoS attacks.

DefensePro not only blocks the attacks, but also provides the best quality of experience to legitimate users during the attack, thanks to its accurate distinguish between attackers and legitimate users.

With its unique detection and mitigation phases and the four escalation steps, DefensePro provides the industry-first complete solution for blocking DNS DDoS attacks from hurting the DNS critical infrastructure.