radware

Protecting Critical DNS Infrastructure

Whitepaper

SHARE THIS WHITEPAPER

Table of Contents

Introduction

DNS is critical Internet infrastructure; every web transaction involves a DNS service provided by an Internet service provider. An 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, which are becoming ever more sophisticated and difficult to mitigate. Therefore, securing DNS service requires rethinking perimeter security—incorporating dedicated tools to identify and mitigate these new breeds of attacks on DNS services.

This paper describes recent DDoS attacks on DNS services and the challenges in mitigating those attacks. It presents Radware's DDoS DNS attack-mitigation solution and its unique differentiators, which make it the best mitigation tool for DNS-service attacks.

DNS DDoS Attacks Are Growing and Evolving

DNS is a critical infrastructure component in any organization. Every web transaction involves a DNS query for name-to-IP-address resolution prior to accessing the requested website. Degrading or even shutting down a service provider's DNS service has an immediate impact on Internet-based services, and can result in blocking legitimate users from accessing the Internet. Attackers understand that service providers take security measures to protect their DNS infrastructure. Therefore, in recent years, attackers have been generating more sophisticated attacks with increased impact on the service.

In the past, large DDoS floods, and in particular large DNS floods, were typically carried out by amplification and reflection techniques. In recent years, with the proliferation of the Internet of things (IoT), attackers can easily take over insecure devices to form a large IoT botnet. With a large botnet of smart devices under their control, attackers can now invest in sophisticated attack vectors in the application layer and specifically in DNS.

One example is the Mirai botnet, which was first used in October 2016 to launch a massive DDoS attack using the DNS random-subdomains attack technique (named by Mirai as "DNS Water Torture"). Since Mirai, there has been a flourish of new and improved IoT botnets, which are growing daily. While these new IoT botnets have not (yet) been linked to any known attacks, they still constitute a risk for the next big DDoS attack.

The following sections describe the main attack techniques deployed by attackers aiming to disrupt the DNS service:

- DNS Flood Attack
- DNS Recursive Attack
  (Random Subdomains Attack)
- DNS Amplification Reflective Attack

DNS Flood Attack

Utilizing multiple sources of compromised computers, called botnets, the attacker generates a distributed volumetric denial-of-service attack, which floods the DNS server. According to the DNS standard, a DNS server processes every request, which results in an overload of the DNS server. This behavior allows the attacker to successfully

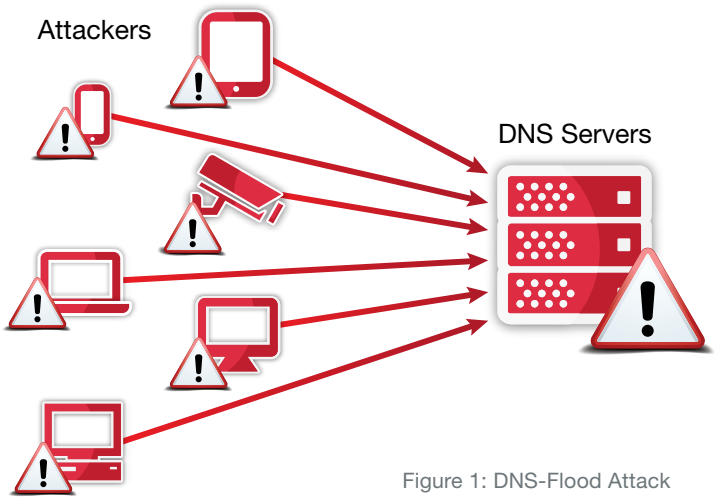

Figure 1: DNS-Flood Attack

compromise the DNS service utilizing a surprisingly small amount of botnets. In addition, spoofing the source IP address is easy, since DNS is typically carried over UDP.

In a basic DNS-flood attack, the botnet spoofs the source address and generates a distributed, volumetric flood composed of the same repetitive fully qualified domain name (FQDN) or multiple FQDNs.

DNS Recursive Attack (Random-Subdomains Attack)

This is a sophisticated DNS-flood attack, where the attacker generates a distributed, volumetric flood towards the DNS servers, composed of random subdomains of a single (or multiple) target domains. In this type of attack, the attacker sends a precrafted DNS query to the DNS recursive server. The precrafted DNS query contains a random string prepended to the victim's domain (for example, xxxyyyy.www.VictimDomain.com). The DNS recursive server will repeatedly attempt to get an answer from the authoritative name server with no success. Sending different false subdomains with the victim's domain name will eventually increase the DNS recursive server's CPU utilization until it is no longer available. In addition, the victim authoritative DNS server will become overloaded by a flood of false requests.

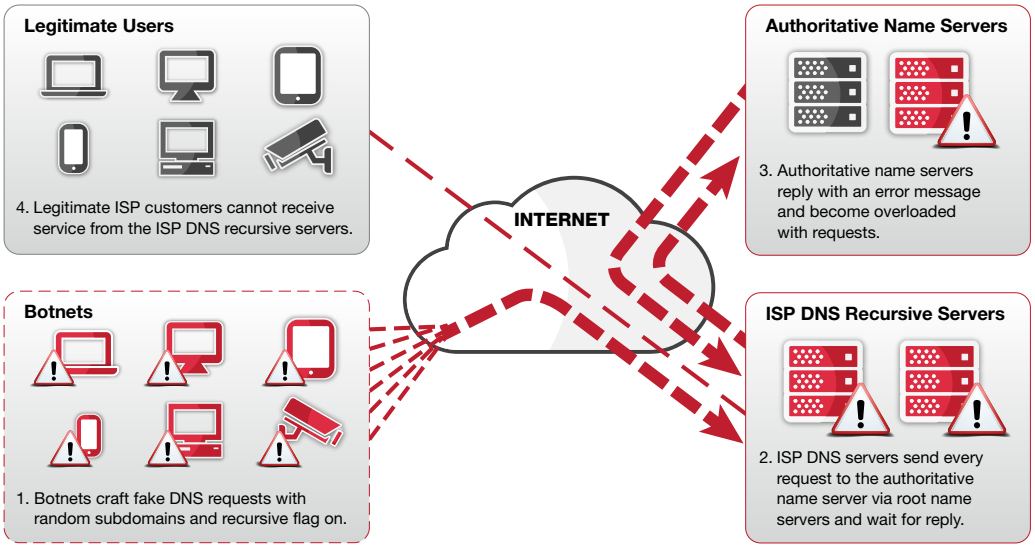

Figure 2: DNS Recursive Attack (Random-Subdomains Attack)

DNS Amplification Reflection Attack

A standard DNS request is smaller than the DNS reply. In a DNS amplification attack, the attacker carefully selects a DNS query that results in a lengthy reply, which is up to 80 times longer than the request (for example: ANY). The attacker sends this query using a botnet to third-party DNS servers, spoofing the source IP address with the victim's IP address. The third-party DNS servers send their responses to the victim's IP address. With this attack technique, a relatively small botnet can carry out a volumetric flood of large responses toward the victim, thus saturating its Internet pipe.

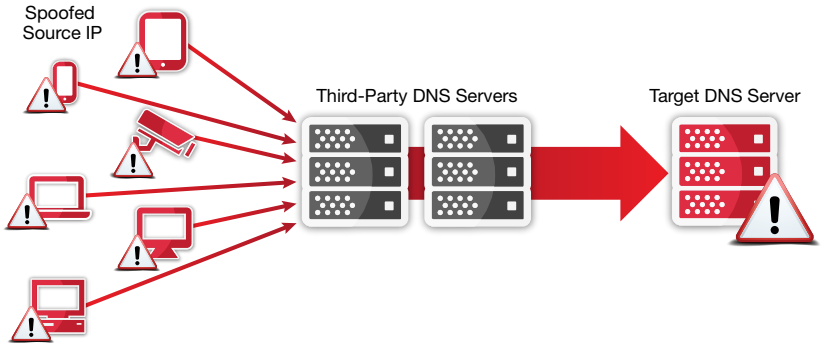

Figure 3: DNS Amplification Reflection Attack

Challenges of Protecting DNS DDoS Attacks

As described above, sophisticated attackers take advantage of the DNS-protocol behavior to generate more powerful attacks.

This section describes the special challenges that today's attack-mitigation tools must be able to meet to successfully block DNS attacks.

Mitigation Tools Must Have Deep Knowledge of DNS-Traffic Behavior

Sophisticated attackers take advantage of the DNS-protocol behavior to generate more powerful attacks, such as the DNS recursive attack (random-subdomains attack). These attacks have greater potential to hurt DNS service. To mitigate such attacks, every single field in the DNS protocol must be carefully analyzed, utilizing a deep knowledge of the DNS protocol and a solid understanding of the DNS-traffic behavior.

Early and Accurate Detection

An indication of suspicious DNS activity is often evident only when DNS error responses (for example, NXDomain) are received. Detection of DNS attacks based on the DNS error responses is often too late for the DNS server, which has already failed due to resources being exhausted. Early and accurate detection of a DNS attack based on the incoming queries alone is a key advantage for true DNS DDoS protection.

Accurate Mitigation

Failure to distinguish between legitimate DNS queries and attack DNS queries results in false positives. The impact of false positives on the Internet service provider is significant, including reputation degradation and loss of revenue. Therefore, today's mitigation tools must be accurate and enable the Internet service provider to provide service to legitimate users even when under attack.

Mitigating High Rate of DNS Packets

DNS DDoS attacks involve a large volume and high rate of flood packets. In order to block all attack packets, the mitigation device must be able to process a high volume of traffic, usually several million packets per second, while still providing enough bandwidth to process legitimate DNS traffic. To achieve high mitigation capacity, the mitigation solution must be stateless, meaning it must avoid keeping any state of the DNS session.

Provide Best Quality of Experience, Even Under Attack

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

Radware Solution for DNS DDoS Attacks

The Radware solution for DNS DDoS-attack protection is based on the DNS behavioral protection modules in its DefensePro product line.

The DNS attack-mitigation solution can be divided into the following three phases described below:

- Detection Phase
- Characterization Phase (Creating a Real-Time Signature)
- Mitigation Phase

Detection Phase

During the detection phase, DefensePro monitors all inbound DNS traffic and learns the baseline of normal DNS traffic behavior. To ensure high detection accuracy, DefensePro monitors both rate and rate-invariant parameters. For each DNS query, DefensePro updates the baselines per query type, query rate, and query name. DefensePro also analyzes the query-type distribution and the query-name distribution. DefensePro uses a stateless positive protection model to learn the legitimate DNS traffic in peacetime.

The DNS attack-mitigation engine continuously generates a degree-of-attack score, using a fuzzy-logic engine. The fuzzy-logic module is a multi-dimensional decision engine, which detects attacks in real-time, based on evaluation of real-time network and DNS data with learned baselines.

When the degree-of-attack score exceeds the value that is considered an attack, the system moves to the characterization phase.

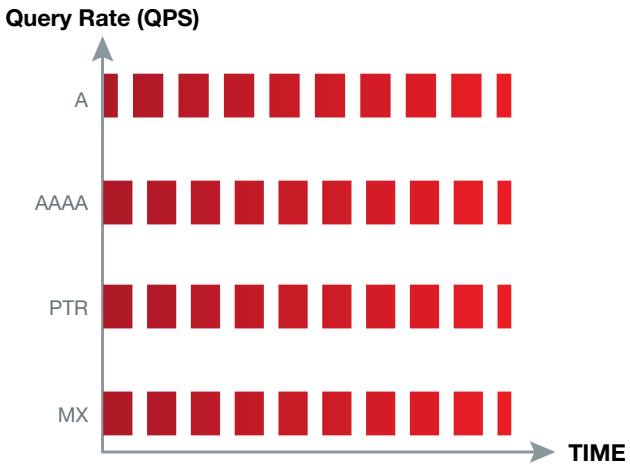

Figure 4: Rate Analysis per DNS Query Type

Characterization Phase (Creating a Real-Time Signature)

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

The parameter types that the automatic-signature-creation module analyzes include the following (among others):

- Packet checksums
- DNS Qname – domain name
- Source IP address
- Packet Identification number
- Identification number
- Port numbers
- Fragment offset
- Packet size
- DNS Query ID – query
- Destination IP address
- TTL (time to live)
- DNS Query count (Qcount)

The real-time signature can accurately identify a query flood on a target FQDN (for example, “www.google.com”) or a recursive flood on a target domain within the FQDN (for example, “google.com”). This unique granularity in the real-time signature ensures accurate and automatic mitigation of all types of DNS attacks.

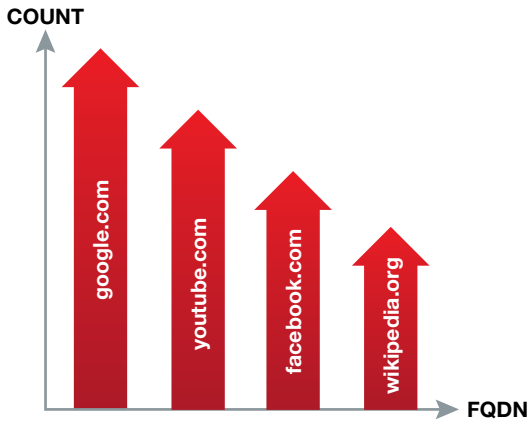

Figure 5: FQDN Analysis per Query Type

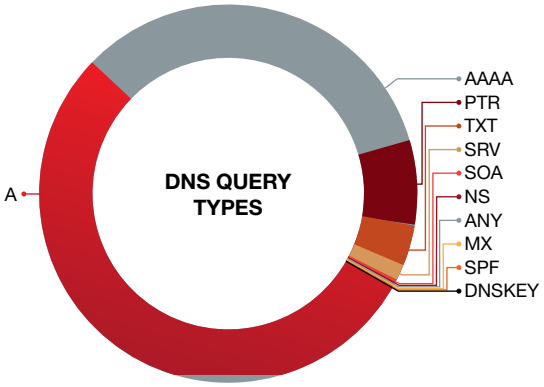

Figure 6: DNS Query Type Distribution Analysis

Using the parameters listed above, DefensePro creates the narrowest-but-still-effective signature-blocking rule. The real-time engine "knows" how to tailor these values through logical relationships (for example: AND, OR).

The engine tests various combinations and performs optimization using the following feedback cases:

- **Positive feedback** – The degree of the traffic anomaly was reduced due to the blocking signature rules created by the module. The system continues to use the same action and tailors more attack-characteristic parameters (that is, signature types and values), through as many logical relationships as possible.
- **Negative feedback** – The degree of the traffic anomaly was not changed, or it 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, the system stops all countermeasures immediately (that is, the system removes the signature rule).

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

Mitigation Phase

During the mitigation phase, DefensePro utilizes the real-time signature to identify the DNS attack traffic and automatically performs *escalation* steps to stop the attack.

The goal of the escalation process is to ensure accurate mitigation and minimize impact on user experience under attack. The escalation steps for a DNS attack are as follows:

1. **Real-Time Signature Challenge** – DefensePro challenges DNS 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.
2. **Real-Time Signature Rate Limit** – If the attack continues, DefensePro limits the rate of DNS traffic that matches the real-time signature.
3. **Collective Challenge** – If the attack continues, DefensePro challenges all DNS-query 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 botnets.
4. **Collective Rate Limit** – If the attack continues, the last resort, and the last escalation step, is to impose a rate limit on all DNS traffic according to the specified maximal query rate.

DNS Challenge—Allow Only the 'Good' DNS Sources

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. The challenge is more effective for a DNS recursive server, which communicates with DNS clients, as opposed to the DNS authoritative server, which communicates with DNS recursive servers.

There are two types of DNS challenge:

- **Passive 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 a limited timeslot containing the same Qname.
- **Active challenge** – DefensePro uses the truncate bit in the DNS header to force the DNS client to switch to TCP. According to the DNS standard, the client must reply over TCP with the same query originally sent over UDP.

The DefensePro challenge verification is done using an advanced scoring mechanism 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. The SDM also implements special treatment for proxy devices, either as legitimate or as attacking devices.

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

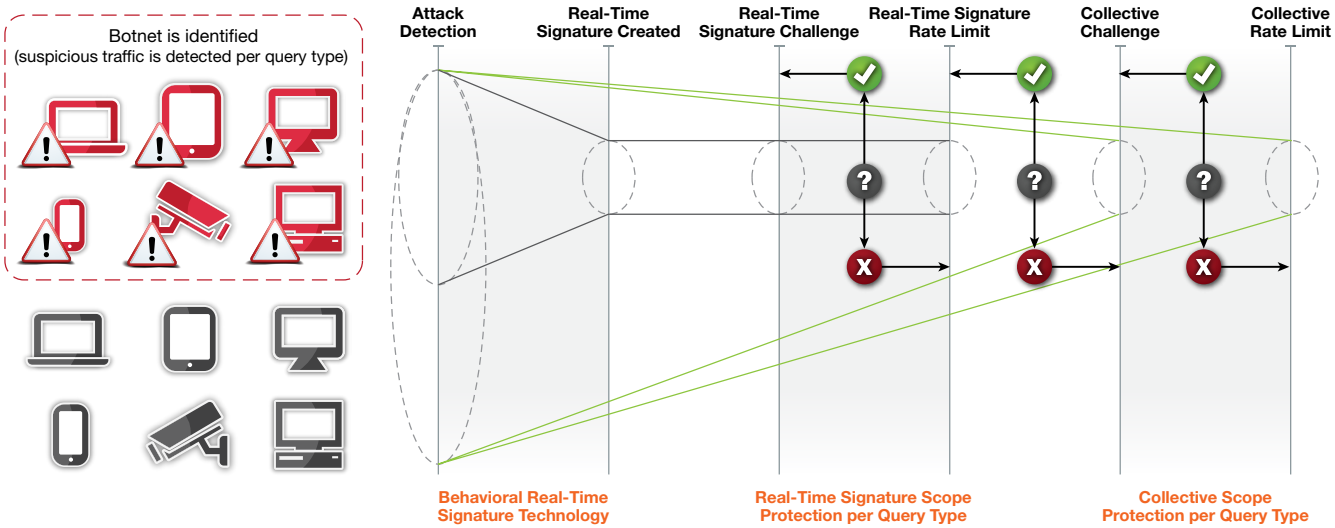

Figure 7: DNS-Challenge and Action-Escalation Process

The DNS Subdomain Whitelist—Allow Only the "Good" DNS Queries

For accurate mitigation of a DNS attack, DefensePro must distinguish between "good" (legitimate) and "bad" (attack) DNS queries. This is essential for accurate mitigation of a recursive random-subdomains attack.

As explained above, DefensePro uses a positive protection model to learn the legitimate DNS traffic in peacetime. DefensePro also uses a real-time signature technology to accurately identify the target domain, within the FQDN, under attack. With these two unique capbailities, when under a DNS recursive subdomains attack, DefensePro is able to allow only the good DNS queries, while blocking the bad queries.

For example, consider a recursive attack on the target domain "example.com." DefensePro will automatically identify the target domain being "example.co." Then, in the mitigation phase, DefensePro will allow only the good, legitimate subdomains of "example.com" to pass through, as well as other domains that are not under attack—while blocking all bad, random subdomains in the incoming queries to "example.com." The detection and mitigation is based only on ingress DNS queires, without the need to wait for NXDomain responses from the authoritative name server.

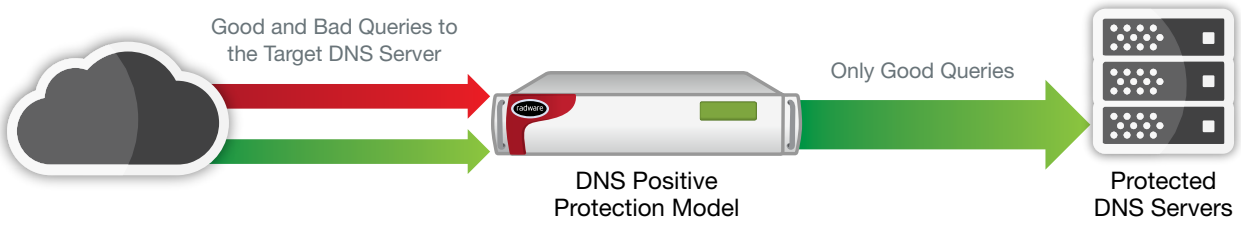

Figure 8: Automatic and Accurate Mitigation Based on Stateless and Ingress-only Technology

DefensePro Meets the Challenges of DNS DDoS Mitigation Tools

As described above, there are several unique challenges that DNS DDoS mitigation tools must meet in order to efficiently and successfully block attacks.

DefensePro is the industry's 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, continually learns its normal behavior, and therefore can immediately identify 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.
- **Early and accurate detection** – The DefensePro DNS solution is designed especially for ingress-only protection. The DefensePro DNS solution is able to learn traffic statistics, then detect and mitigate DNS attacks solely based on the DNS queries coming into the protected DNS server. This is a key advantage, especially in cases of recursive random-subdomains attacks, which can tip over a DNS server handling the fake queries. DefensePro can accurately and automatically detect and mitigate a recursive random-subdomains attack based solely on the incoming queries, without the need to wait for the error responses (for example, NXDomain). The solution is purely stateless; that is, DefensePro does not need to keep any state of the DNS sessions for detection and mitigation of DNS attacks.
- **Accurate mitigation** – With unique DNS real-time signatures, DNS-traffic-statistics collection, and analysis of DNS traffic behavior, DefensePro provides a highly accurate distinction between "good" legitimate DNS traffic and "bad" attack DNS traffic. This results in minimal false positives and enables the service provider to continue to serve its legitimate users, even under severe attack.
- **Mitigating high rates of DNS packets** – Utilizing its *DoS Mitigation Engine* (DME), a network–processor-based hardware accelerator, DefensePro can achieve high mitigation capacity without impact on legitimate traffic processing. The DefensePro DNS protection engine is stateless, similar to other DefensePro engines. Not keeping the state is a key requirement for a DDoS mitigator that is situated on the perimeter, protecting against high-volume floods.
- **Provide best quality-of-experience, even under attack** – DefensePro has a unique architecture that is based on several hardware engines and accelerators. This architecture guarantees a minimum latency to all processed traffic, and especially to legitimate traffic. DefensePro applies the mitigation actions (described above) only to sources that the real-time signature suspects as sending attack traffic. This guarantees the best quality-of-experience to legitimate Internet users, even under attack.

Summary

DefensePro is the best mitigation tool for DNS DDoS attacks, as it provides a unique set of patented tools to successfully mitigate sophisticated, as well as volumetric, DNS DDoS attacks.

DefensePro not only mitigates the attacks, but also provides the best quality of experience to legitimate users during an attack, thanks to its ability to accurately distinguish between attackers and legitimate users, and its ability to accurately distinguish between legitimate and attack DNS queries.

With its unique detection and mitigation phases, based on stateless and ingress-only technology, DefensePro provides the industry a complete solution for protecting the DNS critical infrastructure from DNS DDoS attacks.