、 。

DPtech Technical White Paper on DNS Protection

Hangzhou DPtech Technologies Co., Ltd.

August 2013

I. Overview

1.1 Background

As a fundamental Internet service, DNS plays a pivotal role in safeguarding the normal operation of the Internet. However, on the other hand, as the world's largest and the most complex distributed hierarchical database, DNS is extremely vulnerable to attacks due to its open-ended and complex features, sheer size, and insufficient attention paid to security considerations ever since its inception. The DNS server has become a fragile link in the Internet architecture. The growing number of attacks against DNS in recent years and its increasing impact, as evidenced by the 2009 Storm Incident that paralyzed the network services in many provinces and the notorious 2010 Baidu Domain hijacking, has made DNS system protection one of the primary concerns of network security nowadays.

1.2 Threats to DNS

1.2.1 DNS Flood Attack

DNS Flood attack sends massive DNS query packets to the DNS server, or a huge amount of query packets for domain names that do not exist, keeping the server busy in sending recursive requests to its upper server. It consumes a lot of server resources, eventually resulting in the DNS server's failure in responding to normal DNS requests.

1.2.2 DNS Spoofing

DNS Spoofing is one of the most common DNS security issues. When a DNS server receives a wrong message due to its own design flaws, it will make a wrong domain name resolution, leading to numerous network security issues. There are three common types of DNS spoofing:

1) DNS cache poisoning

A local DNS server cannot verify information from the authoritative DNS server. By exploiting this feature, DNS cache poisoning fabricates fake DNS responses to deceive the local DNS cache. The attacker makes a guess at some features of the communication between the local DNS and the authoritative DNS, based on which he/she forges a large number of response packets. For example, the attacker guesses the DNS response ID. As it is difficult to identify these forged packets for the local DNS, the attacker can send the forged response packets to the local DNS. This process is known as cache poisoning.

2) Session hijacking

Session hijacking occurs when the client initiates a DNS resolution request and is directed to a

malicious website by the attacker who listens to the DNS session, guesses the response ID of the DNS server, and submits a fake response to the client.

3) DNS redirect

After the DNS domain name query request is redirected to a malicious DNS server, the hijacked domain name is completely under the control of the attacker.

1.3 Drawbacks of Current DNS Protection

1.3.1 System expansion

System expansion is an efficient method to address the growing number of visits by improving the ability to process DNS requests per second through enhancing the performance of DNS servers or increasing the number of DNS servers. However, it is far from adequate to rely solely on system expansion in the face of the destructive DNS attacks, given the fact that the request traffic per second reaches up to 10 million QPS.

1.3.2 DNSSEC

Domain Name System Security Extensions (DNSSEC) is a series of DNS security authentication mechanisms provided by the IETF. It provides an extension of source identification and data integrity. Although DNSSEC helps improve the security of DNS systems, it is extremely daunting to fully deploy DNSSEC in a short time. What's more, DNSSEC consumes a lot of resources, which may also become a new hidden danger of DNS.

1.3.3 Firewall

As the firewall itself provides no DNS-specific protection, it can do nothing to guard against diverse DNS attacks.

II. DPtech DNS Protection Technologies

2.1 Technical Overview

DPtech offers a systematic and comprehensive protection solution, aiming at eliminating the drawbacks of traditional DNS protection. The core of the entire DNS protection system is composed of five parts, namely, DNS preprocessing, DNS detection, DNS protection, DNS Cache, and DNS information analysis and statistics. Boasting a variety of services designed for the DNS service system, including security monitoring, eliminating attacks, log analysis, domain name management and monitoring, the DPtech solution enables across-the-board protection and monitoring of the DNS servers.

2.2 DNS Packet Pre-processing

There are some non-conforming DNS packets on the Internet, the domain names of which are too long or contain illegal characters. Although the number of these packets is small, the non-standardized content may also cause unknown security issues to the server. Generally, a DNS protection module cannot distinguish between non-standard packets and normal ones. To this end, a special pre-processing module can be added for filtering and dropping non-conforming packets in accordance with RFC1034, 1035, and 2181.

In addition, DNS access control can also be added to filter the packets by allowing the users to create a whiltelist and a blacklist for domain names, IP addresses and DNS types as needed. For example, IP addresses or domain names that frequently launch attacks can be directly filtered out without going through the subsequent identification and protection modules, thereby improving the overall system efficiency. Similarly, trusted IP addresses or domain names can be directly forwarded to the DNS server for processing without going through the subsequent modules, thereby accelerating user access.

2.3 DNS Detection and Early Warnings

The conventional method of judging whether an attack occurs according to the traffic threshold has its limitations. For example, the normal DNS request traffic generated by some hot issues might exceed the protection threshold configuration, leading to false positives. As another example, the attacker sends DNS requests for some fake domain names, keeping the server busy in sending recursive queries to its upper server and consuming a lot of server resources. However, the traffic of this attack might fall within the threshold, leading to false negatives. The above-mentioned drawbacks are typical in traditional DNS attack detection. DPtech accurately detects attacks in the following two aspects:

1) Real-time analysis of DNS resolution failure rate

The resolution failure rate increases despite the fact the requested domain name does not exist and the server responds with “no such name”, which means there are a large number of unresolvable requests (exceeding the specified threshold), and indicates that there may be an attack. Analysis on the failure rate helps detect attacks even in case of small traffic.

2) Real-time analysis of the ratio between DNS response packets and request packets

If the server is paralyzed by the large traffic generated by the attack, it will fail to provide a response packet, i.e., “no such name” packet will not be generated. In this case, a complementary detection method can be used. When the server is paralyzed and unable to reply, it implies an imbalance of

ratio between the DNS server response packet and the request packet. The smaller the ratios are, the possibility of an attack on the server increases.

The two methods can detect any kind of attacks in the first place and provide a basis for further protection.

2.4 DNS Protection

2.4.1 DNS traffic control per source IP

It supports traffic control per source IP and per source IP range by setting various thresholds for different source IPs. It supports identification and display of source IPs with TOP N page views.

2.4.2 DNS traffic control per domain name

It supports traffic control per domain name by setting various thresholds for different domain names. It supports identification and display of source IPs with TOP N page views.

2.4.3 DNS traffic control per multi-level domain name

The above method cannot protect discrete attacks against domain names. However, upon observation, it is discovered that a discrete domain name is by no means completely discrete, but rather partially discrete. For example, .com is a TLD (top-level domain), baidu.com is a SLD (second-level domain), and so forth. Therefore, multi-level protection is performed to make statistics and observation on each domain level. Take attacks targeting at *.baidu.com for example. Traditional full domain statistics does not work for such attacks, but through detection and protection against the second-level domain names, they can be easily detected and dropped. With 8-level domain detection and protection, DPtech solution is capable of effectively protecting against random DNS attacks targeting at sub domains.

2.4.4 TCP Bounce scanning

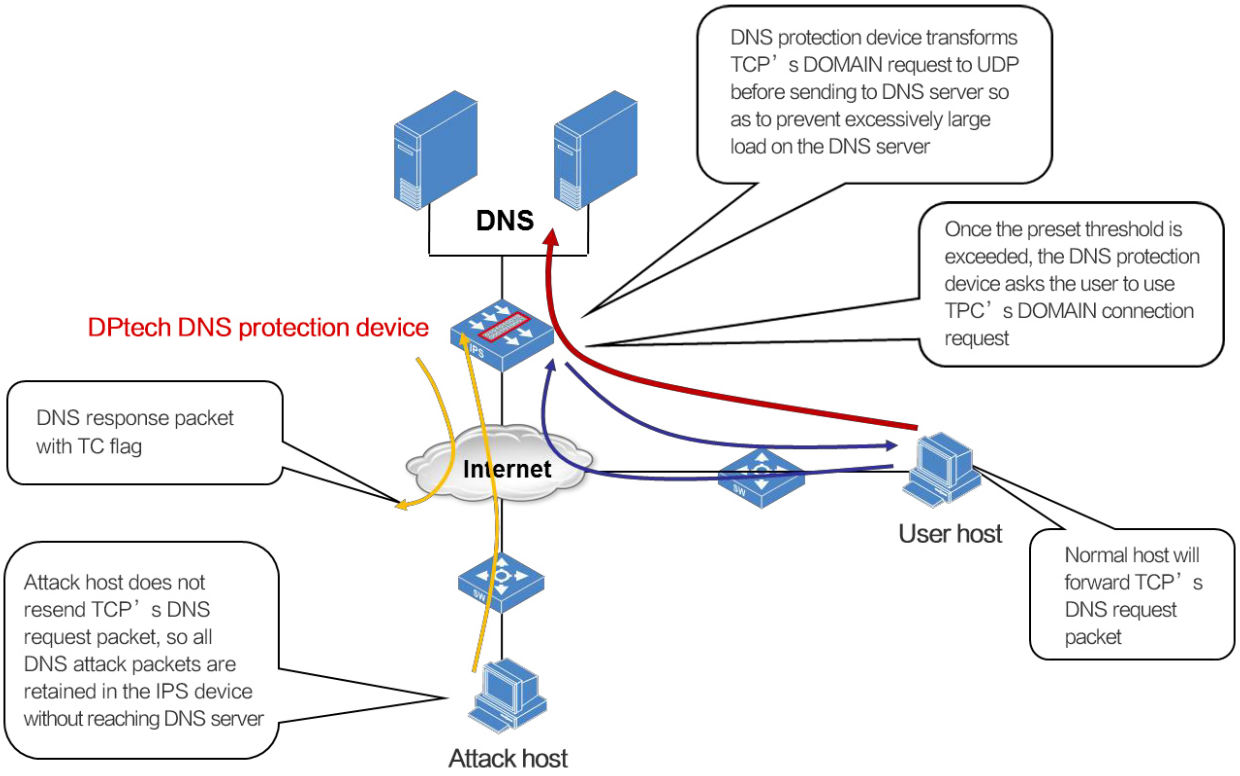


Fig. 1 TCP bounce scanning

Almost all DNS attacks are launched through UDP packets, which provide us an opportunity to protect against discrete DNS attacks. When a DNS attack is detected, the device will return a response packet with the TC flag. In this case, a properly working host will re-initiate a request based on TCP port 53. After receiving the TCP request, the device will convert it into a UDP request before sending it to the DNS server, preventing the DNS server from overloading the server by processing too much TCP packets. However, simulated attack packets sent by the attack software will never resend the TCP packets of DNS requests, so all DNS attacks will be discarded by the device without getting to the DNS server.

2.4.5 DNS Propagation Checker

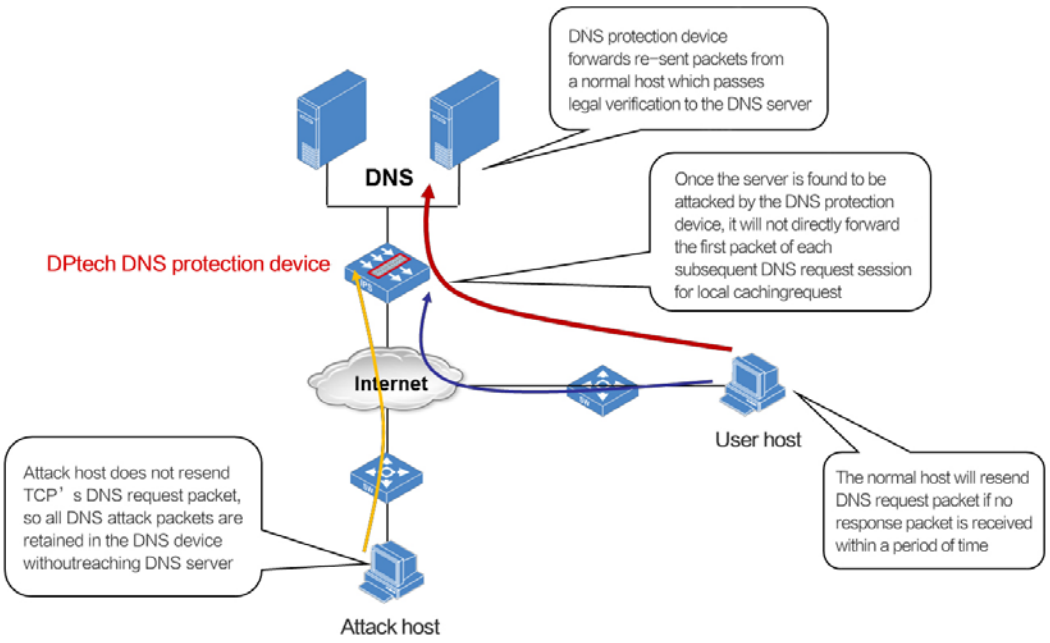


Fig. 2 DNS Propagation Checker

When an attack is detected, the device will cache the first request packet received subsequently locally instead of forwarding it to the server. A properly working host will resend the DNS request packet if no response packet has been received for a period of time (2-5 seconds), but the attack packet will keep sending requests within a short time. Taking advantage of this feature, we can immediately drop attack packets that violate the propagation interval.

2.4.6 Intelligent fingerprint recognition

Any field of the DNS packets can become effective means to detect DNS attacks as both IP address and domain name are random. By performing layer-3 and layer-4 fingerprint recognition on the packets, similar fingerprint features can be identified in these fields, for example, the source port may be identical. Based on these identical features, detection and protection can be performed on DNS request packets to solve the problem of random IP addresses and domain names. As it is hard to make all fields in the attack packets random, the fingerprint recognition method can effectively help protect against DNS attacks.

2.4.7 DNS cache poisoning protection

Upon receiving a request packet, a DNS session is established based on five elements: source IP, destination IP, source port, destination port, and DNS ID. The DNS response packets without any session are deemed as poisoning and discarded. Only response packets with a session can be delivered to the back-end DNS server. It is far more difficult to forge session information than DNS response ID, so it is hard for an attacker to send poisoned attack packets to the DNS server.

In the meantime, thanks to the built-in Cache of the DNS protection device, the DNS resolution is enabled to eliminate wrong resolution results sent by the poisoned DNS server. The two methods combined can effectively protect against cache poisoning.

2.4.8 DNS key domain name monitoring

Focused monitoring and detection can be made on key domain names that are prone to frequent attacks. Upon allocation of these domain names to specified IP address groups, when an IP address changes beyond a specified IP group at a certain time, an alert will be triggered to notify the administrator to check this change and figure out whether a service is under attack. The detection mechanism helps find out DNS Spoofing attacks in time.

2.4.9 DNS response packet filtering

It aims at filtering response packets received by the device according to specified rules. IP addresses in the response packet containing intranet address, special-purpose address, or customized address can be filtered out in the DNS resolution result to maintain normal addresses before forwarding the response packet. If all IPs in the resolution result are illegal, the entire packet will be dropped. In this way, response packets containing illegal addresses cannot reach the DNS server.

2.5 DNS Cache

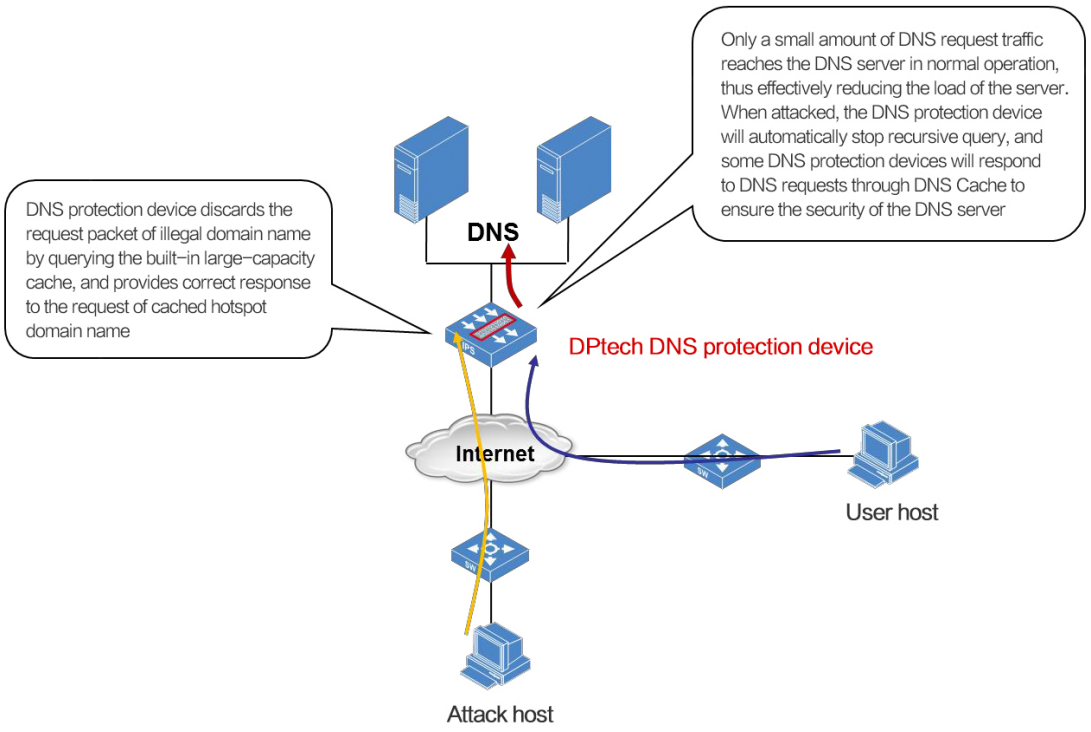


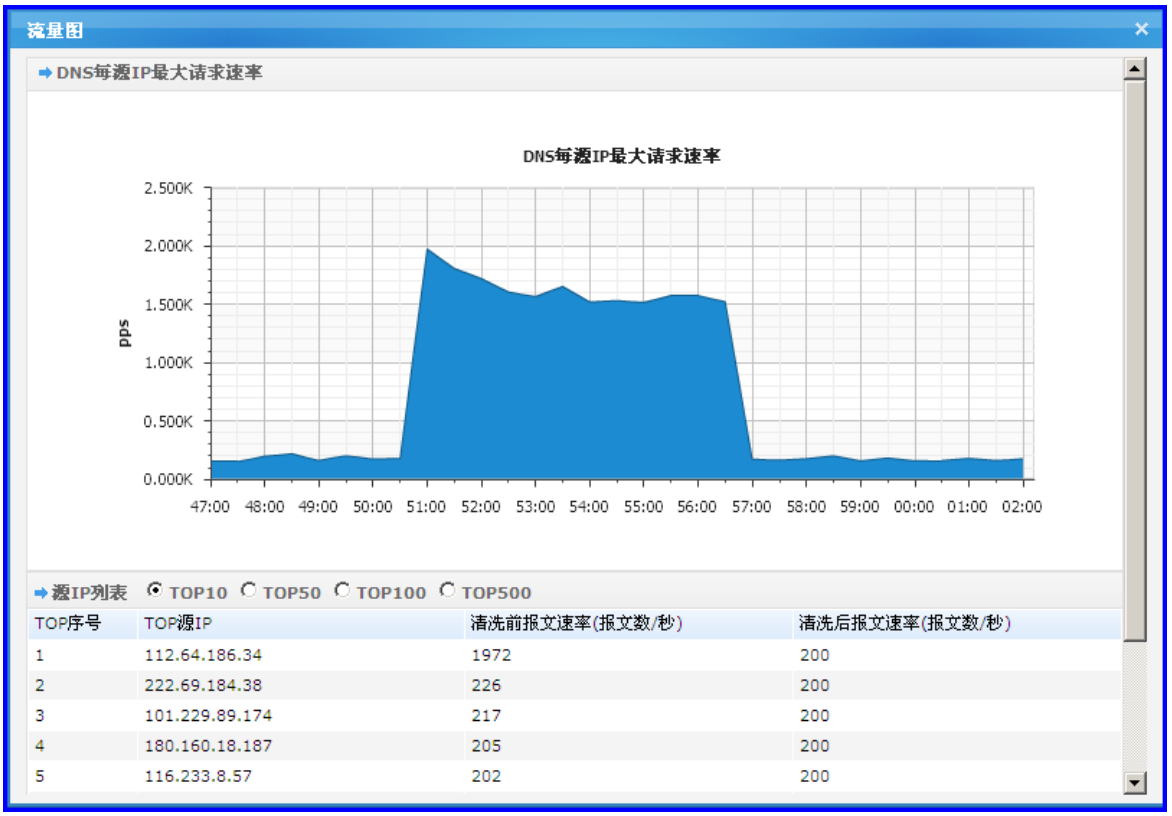
Fig. 3 DNS Cache

As the overall network processing performance of DNS protection device is generally higher than that of the DNS server, the DNS Cache can be used instead of the DNS server for reply, thus greatly reducing the DNS server loads. In discrete DNS attacks, the DNS request packet first matches the entry in the DNS Cache and responds the request in case of any hits, or reports to the DNS server for recursive request in case of no hit. As most DNS requests are replied by the DNS Cache, a large number of recursive requests might be indicative of traffic attacks. In this case, traffic control can be performed on these recursive requests to avoid any potential impact on the DNS server.

The DNS Cache module generally works with the DNS protection module. The DNS Cache module responds to most common requests, and the DNS protection module filters the remaining recursive requests. As a result, traffic reaching the DNS server is small. This not only ensures normal Internet access, but also reduces loads on DNS server.

2.6 DNS Information Analysis and Statistics

A wide array of attack logs and reporting statistics are provided to address DNS abnormal traffic in anti-DDoS products. Information available includes the traffic before attacks and after cleaning, the size, duration and sorting of traffic, attack trend analysis, and other detailed reports to offer users a full understanding of traffic status.



TOP序号	TOP源IP	清洗前报文速率(报文数/秒)	清洗后报文速率(报文数/秒)
1	112.64.186.34	1972	200
2	222.69.184.38	226	200
3	101.229.89.174	217	200
4	180.160.18.187	205	200
5	116.233.8.57	202	200

Fig. 4 DNS statistics and logs per source IP

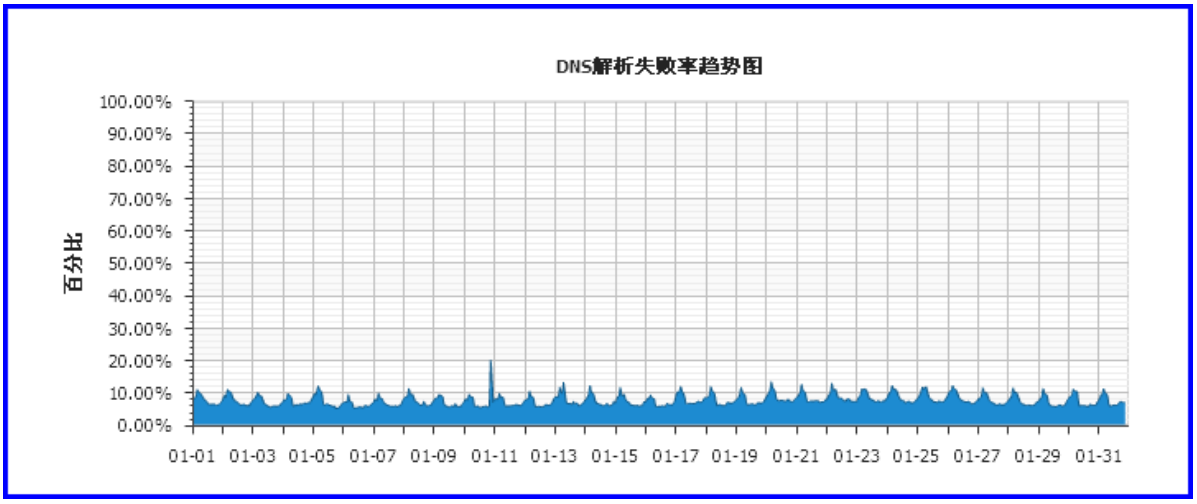


Fig. 5 DNS resolution failure rate

2.7 Other Attack Protections

In addition to DNS attack protection, DPtech DNS protection solution can effectively guard against other conventional DDoS attacks.

2.7.1 ACL Large-capacity hardware ACL

Through configuring the hardware ACL, only required packets are released, such as DNS related packets and management protocol packets responsible for managing SSH packets initiated by management IP, preventing the DNS server from conventional DDoS attacks.

2.7.2 Diverse anti-DDoS technologies

With diverse technologies including SYN Cookie, limiting connections, multi-dimensional traffic control, source IP validity check, protocol behavior detection, and intelligent feature identification of abnormal attacks, DPtech is well-positioned to provide comprehensive anti-DDoS protection against TCP Flood, UDP Flood, SYN Flood, ICMP Flood, etc.