

DNS whitelist against DDoS attack

2011. 2. APTLD

KISA / KRNIC
Yu-Kyung Jung

Contents

- What is DNS whitelist?
- How to make DNS whitelist
- KRNIC Plan
- Consideration
- How to use DNS whitelist

Whitelist

- Whitelist vs. Blacklist
- E-mail whitelist
 - The list of e-mail addresses, domains, and/or IP address which is acceptable
 - To prevent from spam mail
 - If a spam filter keeps a white list, a mail from the list will always be allowed

DNS Whitelist

- DNS whitelist
 - The list of cache name server that access authoritative servers with accurate DNS queries
- Purpose
 - To prevent from DDoS attack

How to make DNS whitelist

- Subscribe for DNS whitelist
- Receive the cache name server list from ISP
- Get IP addresses from DNS queries

KRNIC Test plan

- KRNIC extracted DNS list to make whitelist
 - For 2 weeks
 - Source IP address list up from DNS queries which 13 authoritative servers received
 - List up the whitelist with a certain criteria
 - Check the list whether name server is or not through query in reverse

Test Result

- 13 authoritative servers received from
 - 1167142 IP address
 - Minimum : 1 query
 - Maximum : 349289 queries

But, all IP address in list can't be whitelist

Consideration

- Threshold
 - How to set?
 - Based on average query
- Durability
 - Periodic checks
 - Normal name server ask similar amount of query within a certain period of time

Considerations

- Period
 - How to fix update period
- Check whether name server is or not
 - How to check
 - We tried to query in reserve, but most of name server blocked

Use of whitelist

- We can use whitelist on DDoS attack
 - Response to cache name servers in whitelist
- The road decrease of authoritative name servers
- Sharing the DNS whitelist with ccTLDs