DNS Security and Attack Prevention

A DNS attack is any attack targeting the availability or stability of a network's DNS service. There are many different ways in which the DNS can be attacked, such as DNS cache poisoning, DDoS, DNS spoofing, and so on. This chapter explains the features available in Cisco Prime Network Registrar which help in preventing the DNS security related threats and attacks.

- Prevention of DNS Attacks in Cisco Prime Network Registrar, on page 1

Prevention of DNS Attacks in Cisco Prime Network Registrar

Following features in Cisco Prime Network Registrar help to prevent the DNS security related threats and attacks:

Cache Poisoning

- **DNS cache poisoning prevention**

  A cache poisoning attack can change an existing entry in the DNS cache as well as insert a new invalid record into the DNS cache. This attack causes a hostname to point to the wrong IP address. For more information on handling cache poisoning attacks, see Detecting and Preventing DNS Cache Poisoning.

- **Dynamic allocation of UDP ports**

  The Caching DNS server uses a large number of UDP port numbers. The large number of port numbers reduce the risk of cache poisoning via Birthday Attacks. For more information, see Dynamic Allocation of UDP Ports.

- **Randomization of DNS transaction ID**

  The DNS transaction ID and source port number used to validate DNS responses are not sufficiently randomized and can easily be predicted, which allows an attacker to create forged responses to DNS queries. The DNS server will consider such responses as valid. In Cisco Prime Network Registrar DNS server, the transaction ID and port number are randomized.

- **Randomized query names**

  Domain randomization allows a DNS server to send upstream queries for resolution with a randomly generated query name. A valid name server responds with the query name unchanged and therefore this technique can be used to ensure that the response was valid.

  Cisco Prime Network Registrar supports randomizing upstream queries, but there are some name servers that do not maintain the randomized case. Therefore, if you enable case randomization, you may block

out valid name servers. The *randomize-query-case-exclusion* attribute allows you to create an exclusion list, so that you can continue to use case randomization, but exclude name servers that do not maintain the case but still respond with a valid answer. For more information, see Specifying Resolver Settings.

DDoS Attacks

- **Rate limiting**

  Rate limiting helps the DNS server from being overwhelmed by a small number of clients. It also protects against upstream query attacks against Authoritative DNS servers. This feature helps to mitigate some of the DDoS attacks and prevents the server from being overwhelmed by a small number of clients. It allows you to limit the malevolent traffic. For more information, see Managing Caching Rate Limiting.

- **Smart cache**

  Whenever Authoritative DNS servers face an outage or are offline for other reasons, this could cause issues with being able to reach Internet services that are likely not impacted. Smart caching allows the Caching DNS server to continue to serve the expired data (last known answer) when it cannot reach the authoritative name servers. The Caching DNS server will still continue to contact the authoritative name servers and when the name servers are once again functional, the Caching DNS server will update its expired data. Smart Caching is useful to mitigate network outages and possible DDoS attacks that make the authoritative name servers unavailable. For more information, see Enabling Smart Caching.

- **DNS amplification attack prevention**

  A DNS amplification attack is a popular form of DDoS attack that relies on the use of publically accessible open DNS servers to flood a target system with DNS response traffic. The primary technique consists of an attacker sending a DNS name lookup request to an open DNS server with the source address spoofed to be the target's address. When the DNS server sends the DNS record response, it is sent instead to the target. Attackers typically submit a request for as much zone information as possible to maximize the amplification effect. In most attacks of this type, the spoofed queries sent by the attacker are of the type, "ANY," which returns all known information about a DNS zone in a single request. Because the size of the response is considerably larger than the request, the attacker is able to increase the amount of traffic directed at the target. In Cisco Prime Network Registrar, the *allow-any-query-acl* attribute on the Manage Servers page helps in minimizing the size of the response.

Data Authentication and Authorization

- **DNSSEC in both Authoritative and Caching DNS servers**

  DNSSEC provides origin authority, data integrity, and authenticated denial of existence. With DNSSEC, the DNS protocol is much less susceptible to certain types of attacks, particularly DNS spoofing attacks. Cisco Prime Network Registrar supports DNSSEC in both Authoritative and Caching DNS servers.

  For more information on DNSSEC support in the Authoritative DNS server, see Managing Authoritative DNSSEC.

  For more information on DNSSEC support in the Caching DNS server, see Managing DNSSEC.

- **DNS firewall**

  DNS firewall controls the domain names, IP addresses, and name servers that are allowed to function on the network. The DNS firewall rules can also be set up for specially designated zones on the Authoritative DNS server using RPZ. The RPZ and RR data combined with DNS resolver effectively

creates a DNS firewall to prevent misuse of the DNS server. For more information, see Managing DNS Firewall.

- **Secure DNS server activity with ACLs**

  You can restrict clients to query only certain zones based on an ACL.

  - Restricting Zone Queries—The *restrict-query-acl* attribute on the DNS server serves as a default value for zones that do not have *restrict-query-acl* explicitly set.
  - Restricting Zone Transfer Requests—The *restrict-xfer-acl* attribute filters the zone transfer request to the known secondary servers.
  - Restricting DDNS Updates—The *update-acl* attribute filters DDNS packet from the known DHCP servers.

- **Secure zone transfers and DNS updates using TSIG or GSS-TSIG**

  Zone transfer in secure mode supports both HMAC-MD5 based TSIG and GSS-TSIG. You can add an optional TSIG key or GSS-TSIG keys (see the *"Transaction Security" or "GSS-TSIG " sections in theCisco Prime Network Registrar 10.1 DHCP User Guide*) to the primary server address by hyphenating the entry in the format *address–key*.

DNS Security and Attack Prevention