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

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

Cache Poisoning

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 and source port**

  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.

- **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

In a distributed denial-of-service attack (DDoS attack), the incoming traffic flooding the targeted server, service, or network originates from many different sources. This effectively makes it impossible to stop the attack simply by blocking a single source.

- **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 Smart Cache settings.

- **DNS amplification attack prevention**

  A DNS amplification attack is a popular form of DDoS attack that relies on the use of publicly 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.

  For more information on security events settings in the Caching DNS server, see Logging Security Events.

  For more information on security events settings in the Authoritative DNS server, see Security Events Settings.

- **Allow ANY Query ACL**

  In Cisco Prime Network Registrar, the *allow-any-query-acl* attribute on the Manage Servers page helps in minimizing the size of the response. This attribute is present in both Authoritative and Caching DNS server pages, and the default value is "none".

- **Minimal responses**

  Cisco Prime Network Registrar supports *minimal-responses* in which authority and additional sections are omitted in the response. This reduces the query response size and defers Denial Of Service to some extent. Starting from Cisco Prime Network Registrar 11.0, *minimal-responses* is enabled on the Caching DNS server by default and is disabled on the Authoritative DNS server by default.

- **Minimised query name**

The behaviour of sending multiple queries can be exploited by sending queries with a large number of labels in the QNAME that will be answered using a wildcard record. For example a record for *.example.com, hosted on example.com's name servers. An incoming query containing a QNAME with more than 100 labels, ending in example.com, will result in a query per label. By using random labels, the attacker can bypass the cache and always require the resolver to send many queries upstream.

One mechanism that may be used to reduce this attack vector is by appending more than one label per iteration for QNAMEs with a large number of labels via Query name minimisation.

Data Authentication and Authorization

- **DNSSEC**

  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**

  Caching 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.

- **Cisco Umbrella**

  Cisco Umbrella provides the first line of defense against threats on the Internet, such as phishing and malware. By setting up the Caching DNS to use Umbrella for resolution, you can allow the Cisco cloud service of Umbrella to provide the latest responses for the requested domain/host. For more information, see Configuring Caching DNS to Use Umbrella.

- **Secure DNS server activity with ACLs**

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

  - Restricting Zone Queries—The Authoritative DNS server attribute *restrict-query-acl* limits device queries that the server must honor. The Caching DNS server attributes *acl-query* and *acl-do-not-query* specify IP addresses or subnets that are queried and not queried respectively.
  - 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.
  - Blocking Malicious Client—The *acl-blocklist* attribute blocks requests from clients listed in this access control list. This list can contain hosts, network addresses, and/or other ACLs. Request from clients matching this ACL will be dropped.

- **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 Cisco Prime Network Registrar 11.2 DHCP User Guide*) to the primary server address by hyphenating the entry in the format *address–key*.

- **Secure queries with DoT**

  DNS over TLS (DoT) is a security protocol for encrypting and wrapping DNS queries and answers via the TLS protocol. It improves privacy and security between clients and resolvers. It uses TCP as the basic connection protocol and layers over TLS encryption and authentication.

  For more information on TLS settings in the Authoritative DNS server, see the Sepcifying TLS Settings section in the "Managing Authoritative DNS Server" chapter.

  For more information on TLS settings in the Caching DNS server, see the Sepcifying TLS Settings section in the "Managing Caching DNS Server" chapter.