White paper
Cisco public

Prime Network Registrar

PNR 11.0 DNS Cache Security Features

Contents

This document is focused on security that can be enabled on the PNR DNS Caching Server. Some references are made to Authoritative DNS as well where that functionality is common across the two.

1.1 Introduction

Cisco® Prime Network Registrar (PNR) 11.0 continues the buildout of security features for DNS. The Domain Name Service is the core for addressing, and therefore accessing, servers and content on the internet. Without DNS, most of the internet accesses break. Furthermore, as seen by the Facebook outage of October 4, 2021, even the outage of one very popular destination can cause a ripple down to impacting other subscriber services as the DNS systems at the internet service providers have to deal with overloads caused by huge numbers of retries and failure messages.

Service providers can mitigate the effects of outside outages and malicious DNS usage by deploying the DNS Cache. The DNS architecture relies upon caching in order to scale. It is the first line of defence for answering common DNS queries, for improving latency in DNS responsiveness, and for defending against attacks.

The following security protections are available on the PNR DNS Cache offering. This information has been summarized from the product manuals. Additional information is available in the manuals.

1.2 Protection against cache poisoning attacks

A cache poisoning attack can change an existing entry in the DNS cache or can insert a new invalid record into the DNS cache. This attack causes a hostname to point to the wrong IP address.

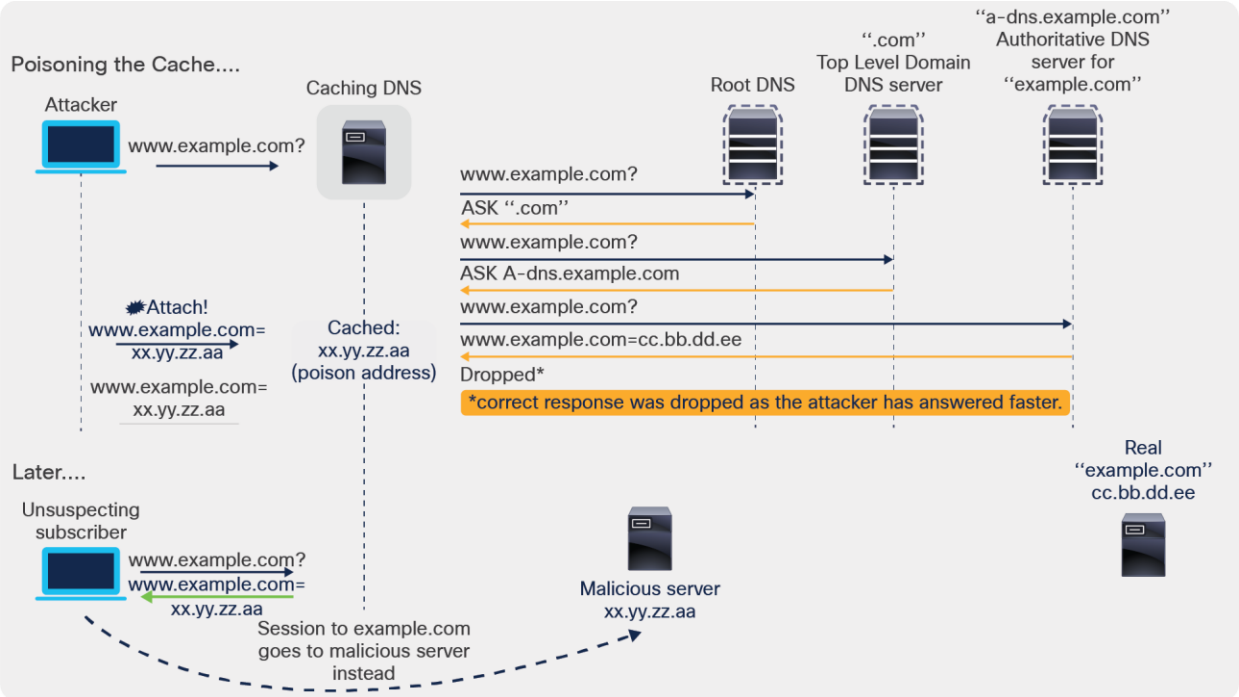

Figure 1.
DNS cache poisoning - How it is done

At its simplest level, to protect against cache poisoning, a resolver implementation must match responses to the following attributes of the query:

- Remote address
- Local address
- Query port
- Query ID
- Question name (not case sensitive)
- Question class and type, before applying DNS trustworthiness rules (see [RFC2181], section 5.4.1)

  Sample metrics for monitoring: ‘answers-unwanted’

Making the protection against cache poisoning more robust, PNR also implements the following protections.

1. 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. In a Birthday Attack, the attacker is trying to guess the UDP Port, pretending to be an authoritative DNS, to which to send a fake (poison) response. By using a large pool and randomizing the source ports for every query outbound for forwarding requests, PNR offers an additional protection against cache poisoning.

2. Randomization of DNS transaction ID

If the DNS transaction ID used to validate DNS responses is not sufficiently randomized, they can easily be predicted, which allows an attacker to create forged responses to DNS queries. The DNS server would consider such responses as valid. By randomizing the transaction ID, PNR makes the attacker’s ability to simply guess a correct value much more difficult.

3. 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. 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 bypass randomization for those servers that do not support it. For more information, see Specifying Resolver Settings.

With these additional protections, PNR can catch and avoid more cases of cache poisoning. The fake response is dropped, and the correct response from the proper DNS authority is retained:

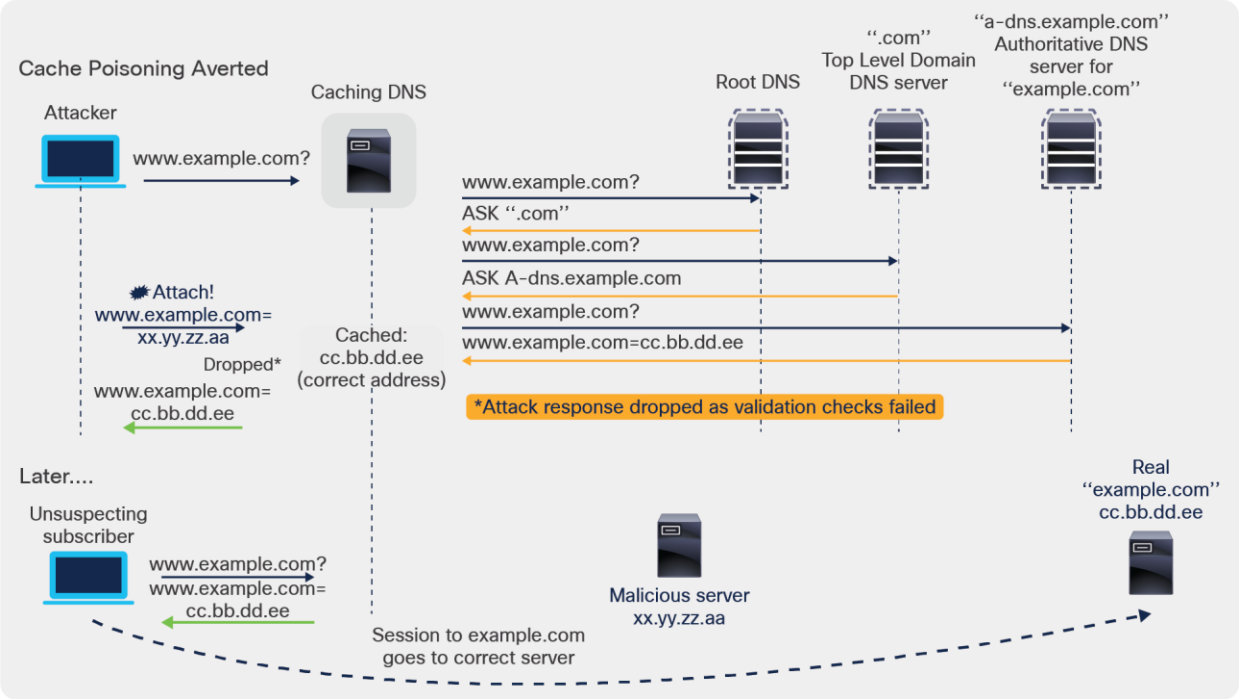

Figure 2.
DNS cache poisoning - Averting the attack

1.3 Protection against DDoS attacks

In a Distributed-Denial-of-Service (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. PNR can rate limit based on either the source (that is, the clients) or by the domain being queried. For more information, see Managing Caching Rate Limiting.

Sample metric for monitoring: 'domain-rate' and 'client-rate-limit'

- **DNS amplification attack prevention**

Unlike other attacks that rely on flooding a DNS system with a high number of queries, a DNS amplification attack is a 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 address of the intended victim. When the DNS server sends the DNS record response, it is sent instead to that target. Attackers typically submit a request for as much zone information as possible to maximize the amplification effect, or can send multiple requests, all indicating to return the responses to the victim. The objective is to flood the victim with large responses or an avalanche of unexpected responses. In most attacks of this type, the spoofed queries sent by the attacker are of type “ANY,” which returns all known information about a domain 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. To protect against this, PNR offers the following capabilities:

1. **Dropping responses for which the DNS Cache did not have an outstanding query**

   If the DNS request was sent by an attacker via a different DNS resolver from the one used by the intended victim, then by ignoring (dropping) DNS responses that did not match a query, the PNR cache engine serving the victim’s DNS avoids processing data for which it had no interest.

   Sample metric for monitoring: ‘answers-unwanted’

2. **“Allow ANY Query ACL” attribute**

   In Cisco Prime Network Registrar, the allow-any-query-acl attribute helps in avoiding queries for type=ANY records. A type=ANY DNS query is used to get all DNS records available for a specific domain name. Such queries are typically considered a security issue, as they can be used in an amplification attack in that a small request can generate large responses if there are many records on a name. The attacker may do this either by creating his own domain with this type of large record or may use one that is known.

   This attribute is present in both Authoritative and Caching DNS server pages, and the default value is "none" (meaning that PNR will block type=ANY queries).

   Sample metric for monitoring: ‘queries-type-any’

3. **“Minimal responses” attribute**

   Cisco Prime Network Registrar supports minimal-responses in which authority and additional sections are omitted in the response when not required. This reduces the query response size and defers denial of service to some extent. It also reduces the number of lookups required, therefore providing a positive effect on performance. As of 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.

1.4 Protecting against malware, data exfiltration, and undesirable content

- **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.

Sample metrics for monitoring: 'firewall-dropped,' 'firewall-redirected,' 'firewall-refused,' 'firewall-redirect-nxdomain,' 'firewall-rpz'

- **Cisco Umbrella**

Cisco Umbrella® protects the subscriber population against malicious or undesirable content, such as phishing and malware. Cisco Umbrella maintains a database of known 'bad' sites, which is updated regularly. The Cisco PNR Caching DNS engine can take advantage of this by using Umbrella for resolution and 'learns' these bad sites by caching the results. The results are learned on a domain basis (not a subscriber basis) and are cached based on their TTL. For more information, see Configuring Caching DNS to Use Umbrella.

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 and cache poisoning 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.

Sample metrics for monitoring:

For tracking queries inbound to the CDNS:

- 'queries-with-edns-do' (note that the equivalent for the PNR Authoritative DNS is 'queries-dnssec')

For tracking responses received by the CDNS:

- 'answers-secure' reports number of answers that were validated with DNSSEC
- 'answers-unsecure' counts queries where the response fails DNSSEC validation and returns SERVFAIL
- 'answers-rrset-unsecure' reports number of RRsets that failed DNSSEC validation

- **Secure DNS server activity with ACLs**

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

  - Restricting queries—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 and restrict-xfer-acl attributes, used together, allow filtering of zone transfer requests to the known secondary servers.
  - Restricting DDNS updates—The update-acl attribute filters DDNS packets from the known DHCP servers and/or known DNS update clients.
  - 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.

  Sample metrics for monitoring: 'queries-failing-acl'

- **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.

- DNS over TLS (RFC 7858) is supported on both the PNR Authoritative DNS as well as the PNR DNS Cache Engine.
- At the Cache, DoT can be configured separately for incoming client requests or for outgoing DNS server requests.

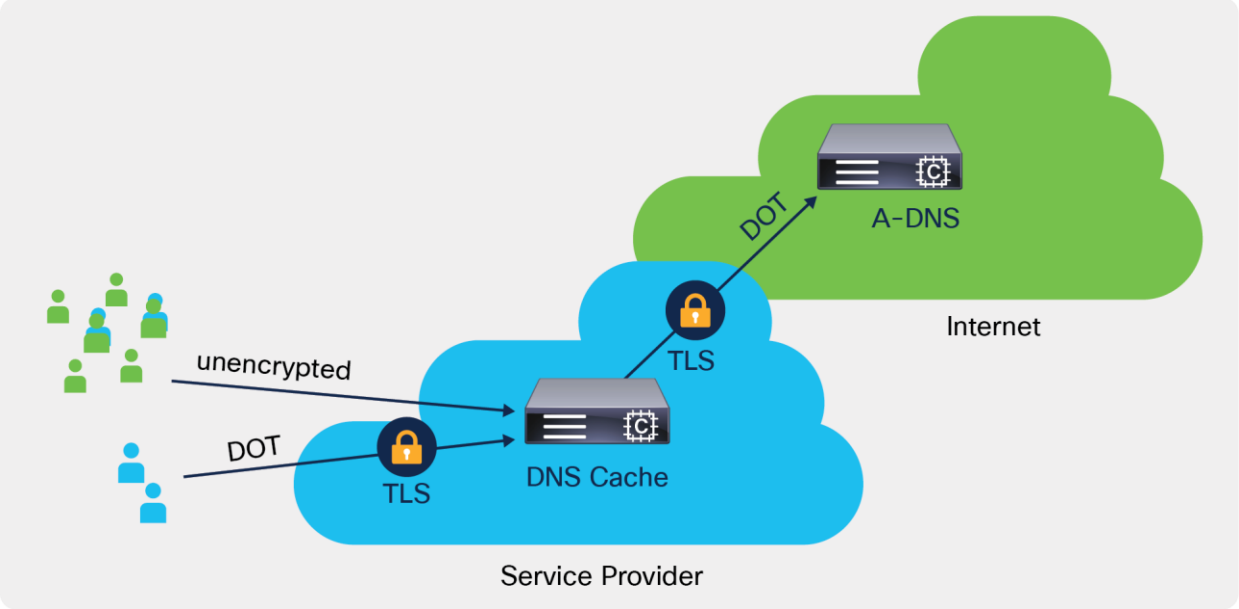

Figure 3.
DNS over TLS

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

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

Additional PNR Features for DNS continuous operation:

- Smart cache

Smart cache is a continuous availability feature that can help a DNS Cache deployment continue to provide service to clients during times when the DNS for the destination domain is unavailable (for example, if the DNS at the destination domain is under attack). 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 (using an exponential backoff to avoid excess outbound queries), 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.

Sample metrics for monitoring: ‘smart-cache.’ When the smart-cache feature is enabled, this metric reports the total number of times the CDNS Server employed a smart-cache response.

Summary

The Domain Name System is an open protocol and has been subject to considerable abuse. The Cisco Prime Network Registrar product offers a number of security features to help protect against attacks and fraud. Although this paper has focused on our DNS Caching Server, similar protections are available also when the product is deployed as an Authoritative DNS. These features have grown over the years with the product, and as shown above, we have continued to provide security features as part of the functionality of our DNS services.

External Marketing Collateral

- Cisco.com landing page: https://www.cisco.com/c/en/us/support/cloud-systems-management/prime-network-registrar/series.html#~tab-models
- Documentation: https://www.cisco.com/c/en/us/support/cloud-systems-management/prime-network-registrar-11-0/model.html?cachemode=refresh
- Product training: Product training can be requested through: https://www.cisco.com/c/en/us/training-events.html

ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENT ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY INFORMATION IN THIS DOCUMENT.

THIS DOCUMENT IS PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C11-2784196-00 01/22