QUANTEA QP CASE STUDY: DNS SERVICES

Quantea
Empowering Data for a Connected World

Overview

Quantea was asked by a major ISP in Japan to help them resolve some issues on their DNS System while being able to use the system 24/7 without causing any interference on the network. Plus, the system had to work with their current security solution by allowing their security system to request information from the Quantea QP at any time.

DNS: Domain Name System

DNS(Domain Name System) is a system that provides a service which enables website names to be translated to IP addresses, and vice-versa through the use of rDNS(Reverse DNS). This system is a massive world-wide database of all domain names and IP addresses associated with those domain names. This allows users to type in domain names and be directed to the website while translating the name into an IP address for the computers to understand. Or, if you type in an IP address you will be directed to a website and the domain name will appear in the address bar and replace the IP address.

Without the DNS service, the Internet would be impossible to navigate since it is not possible to know every IP address of every website.

Telecoms, ISPs, and special service providers like Yahoo, Google, Baidu, Bing, and many others have massive, powerful DNS systems in order to provide their services.

DNS Hierarchy:

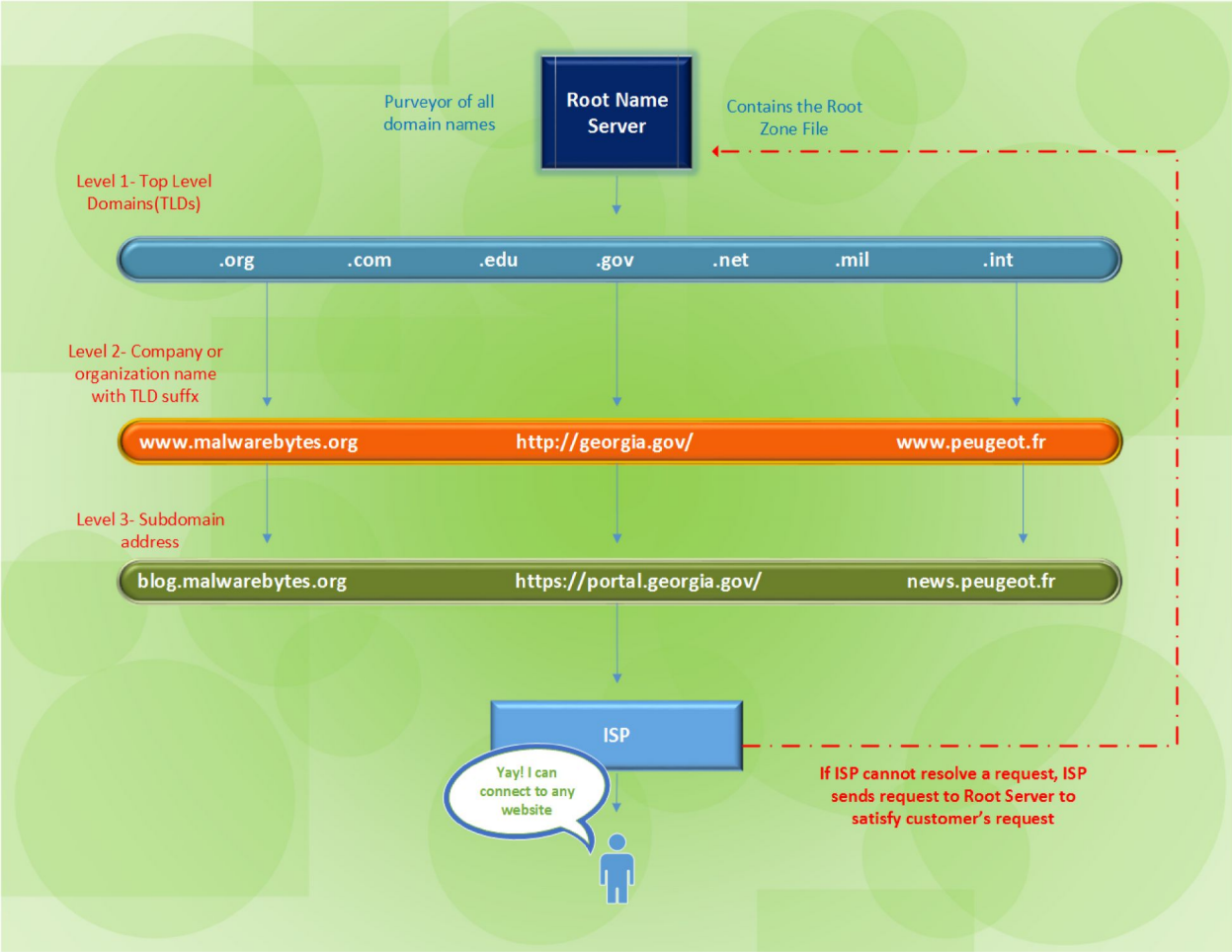
1. At the top of the hierarchical structure of the DNS is a set of clusters of Root Servers, or Root Name Servers that make up the DNS Root Zone. There are 13 total logical root name servers throughout the world which contain the name server information for all of the top level domains(TLDs) like .com, .org. .mil, .net, .edu …and so forth.

   The other top level information contained here is the geographical references of domains in certain countries. These are usually 2 letter identifiers such as; .jp, .uk, .co, .it, .br, .fr …and so forth.

2. The second level of the hierarchy contains the company, or organization name along with its referred TLD suffix. Ex: www.google.com, http://georgia.gov, www.peugeot.fr.

3. The third level includes the subdomain address which commonly includes Support, Blogs, News, Careers, About…
   Ex: blog.malwarebytes.org; https://portal.georgia.gov/; news.peugeot.fr

DNS Hierarchy

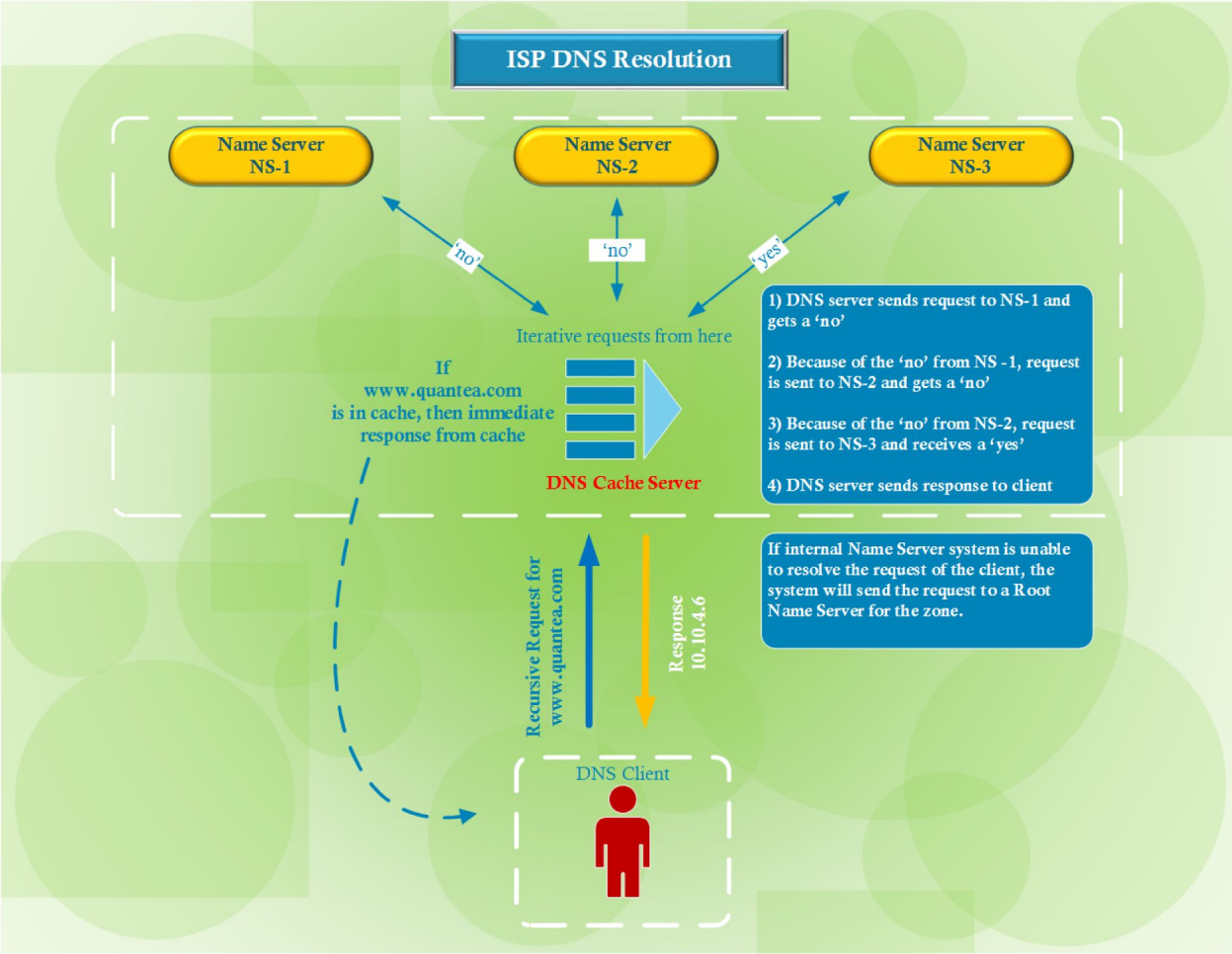


DNS Queries & Resolution:

When a customer connects to the ISP, they send requests for websites to the ISP and the servers and routers in the ISP send these requests to its own DNS cache server and Name Servers, and sometimes have to send a query to a Root Name Server outside of the ISP if it is unable to resolve the requested domain name within its system. When the Root Server resolves the request, the ISP will add this information to its own DNS system.

1. Recursive DNS queries - a DNS client requests information from a DNS server that is set to query subsequent DNS servers until a definitive answer is returned to the client. The queries made to subsequent DNS servers from the first DNS server are iterative queries.

2. Iterative DNS queries - queries in which a DNS server is queried and returns an answer without querying other DNS servers, even if it cannot provide a definitive answer. Iterative queries are also called non-recursive queries.



The Problem

The solution had to be able to capture DNS traffic in such a way that shows every bit of information about what was happening during the DNS query process, while also being able to store the data and able to run analyses on the data.

The main issue for all DNS solutions is that they need to reply to queries quickly and with the correct information. The correct information means that the ISP can resolve the request with the correct address, and hopefully, not direct the end-user to a malicious site. Thus, one of the main problems DNS systems face is Security.

Security Issues:

1. DOS attacks - Servers supporting recursive DNS queries are vulnerable to phony requests that flood a particular IP address with the results of each server's query. This can overwhelm the IP address with a volume of traffic, causing the site/server to crash.

2. Cache Poisoning - the attacker corrupts a DNS server by replacing a legitimate IP address in the server's cache with a re-direct address in order to redirect traffic to a malicious website.

3. DNS amplification – a form of DDoS, the attacker takes advantage of a DNS server that permits recursive lookups and uses recursion to spread the attack to other DNS servers. The system sends requests to the targeted IP address (victim), causing a storm of responses to flood the IP address and shuts the site down.

4. DNS Fast-Flux - is a DNS technique used by botnets to hide phishing and malware delivery sites behind an ever-changing network of compromised hosts acting as proxies. The basic idea behind Fast flux is to have numerous IP addresses associated with a single fully qualified domain name, where the IP addresses are swapped in and out with extremely high frequency, through changing DNS records.

Traffic Analysis:

How do you capture DNS traffic and look at every specific detail of the packet in order to identify the issues, or important traffic information?

This was one of the major concerns for the ISP since their current solution could not capture and do a Deep Packet Inspection with the detail they needed. They needed to be able to look at captured data over a period of time and look at historical bits of information. This information could provide them the ability to see traffic patterns, trends, errors, DNS attacks, and even misconfigured network elements such as routers, switches and DNS servers.

Another issue is that of dropped packets. Yes, packets can be dropped in a DNS query and an error is sent to the client. Through traffic analysis, the ISP can see why, and where, the packets are being dropped.

They also want to see when an address is queried and is not resolved, but directs the client to a default search engine or specific page. They want to be able to tell why it's not being resolved. It may not be a malicious redirect, but rather a request typed incorrectly by the client, or the domain may not exist anymore. There are many possibilities for this, but being able to find the exact reason why, quickly, is of major importance as the ISP has to be concerned with the satisfaction of their customers.

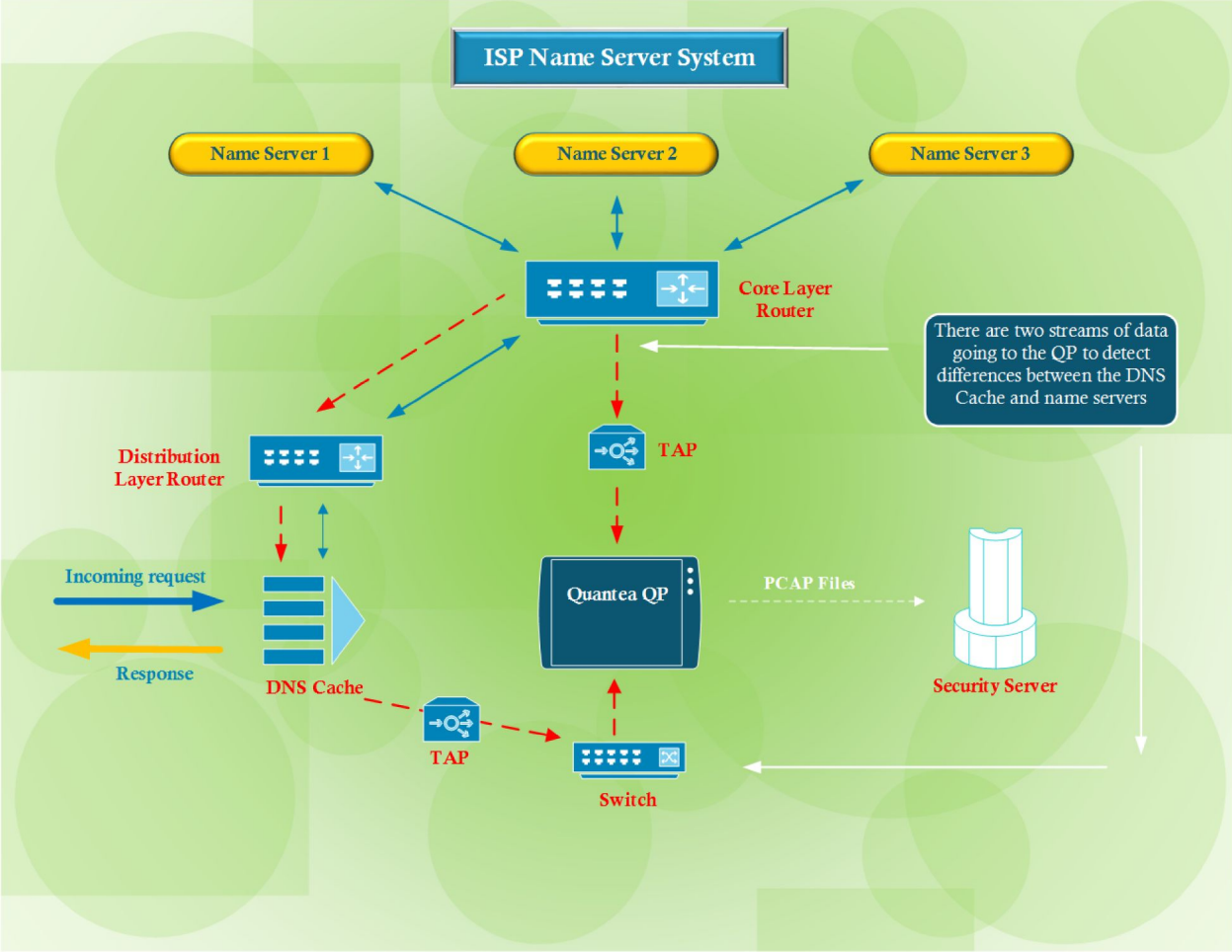
Differences between a DNS cache system and the Name Server can cause many issues for a DNS resolver system. Symmetry between these systems is a key issue that the ISP was concerned about. If the DNS cache is not updated by the Name Servers, then it will always query the Name Servers for the domain name, creating an unnecessary step and extra traffic in the query process.

QUANTEA QP CASE STUDY: DNS SERVICES

The Goals

1. To discover what was causing the issues
2. Achieve symmetry between the DNS Cache and Name Servers
3. Identify DNS attacks
4. Capture data 24/7
5. Be able to retrieve relevant packets in an event of an issue or attack

The Process and Solution



*The QP is processing 90,000 queries/second.

The Quantea QP was strategically placed in the DNS system to capture DNS query and response traffic from two data sources: The DNS Cache Server and the Name Servers.

Quantea
Empowering Data for a Connected World

WWW.QUANTEA.COM
SALES@QUANTEA.COM

QUANTEA QP CASE STUDY: DNS SERVICES

Data Streams:

1. **Name Server response data:** The Quantea QP was connected to a core router through a TAP which mirrored the query response traffic from the Name Servers.

2. **DNS cache data:** Another TAP was placed between the DNS Cache server and a switch connected to the QP. This traffic shows the response to queries from the DNS cache server.

Capturing the two data streams were necessary in order to check the difference between the DNS cache information and the Name Server information. There can be differences between the systems due to misconfiguration, wrong information on the databases and text records, and DNS attacks.

The captured data is stored in PCAP files. The Security server requests the PCAP files in order to run a custom software designed by the ISP to determine the difference between the DNS cache files and Name Server files. The requested files can be obtained from the QP based on a custom search performed by the QP search engine. The data can be chosen based on time, date, size, and data type.

Because the QP captures every detail of the traffic data, the ISP can also do a deep analysis of the PCAP files above and beyond what the Security Server analyzes and use the QP search engine to discover any type of DNS information, anomaly, or attack. Some of the information collected in the PCAP files include CNAME records which need to be inspected because sometimes CNAME records point to other CNAME records which then can lead to unresolved loops. The ISP looks for these anomalies and updates their records and settings to make sure this type of file is avoided along with other CNAME anomalies.

Other DNS records include, but are not limited to: TXT(text record), MX(mail exchange record), A(for IPv4 addresses), AAAA(for IPv6 addresses).

Rolling Data: Because of the storage capabilities of the QP, the ISP was able to capture a couple weeks worth of DNS data to be stored and processed as they wished. That is because the QP system has a Rolling Data capability that allows the customer to set a threshold for the amount of data to be captured and stored. The threshold of the amount of data can be set by the user and the system will automatically delete the old data as new data is added based on FIFO(First In First Out). The compression capability allowed this ISP to store 1PB of data without any problem. This allows the ISP to search and analyze the data, according to their schedule, without worrying about losing the files.

> Example: If the threshold is set at 95%, then the system will delete 5% of old data to maintain a data set of 95% of storage capacity.

Other traffic analysis that is always being done by the ISP is that of traffic patterns and trends during specific times. Peak traffic time analysis can help an ISP to see which domains are being requested the most and they can set their system to resolve requests faster for these specific sites. Such sites may include news channels that people access before and after work, or making sure that YouTube traffic is resolved properly during the 8pm-11pm timeframe. Also with the QP, they can detect purposely misdirected traffic from YouTube to another video site.

Because the QP is a passive device, it was able to collect data streams and process the information without disrupting the services of the network.

QUANTEA QP CASE STUDY: DNS SERVICES

The system described herein worked perfectly 100% and is currently running 24/7. Not only did the ISP discover all issues involved in their DNS system, but also discovered new ways to use the system going forward for other analyses and information gathering to better their service.

Our customer had been reviewing various systems from JDSU(Viavi), Fluke and Netscout for DPI, and both NetApp and Hitachi Data Systems for the storage need. The cost of anyone of these systems can take your breath away and still not provide the features and functions needed. Plus, the ease-of-use capability goes down the drain as soon as you have to combine two systems that are not naturally built for each other and have to use two separate management interfaces.

The Quantea QP solution provided the ISP with everything they needed in a Deep Packet Inspection solution while also providing built-in storage in one system with an easy to use interface.

Key Points

- Discovered all issues
- Reduced time to discover every issue because of the information captured and the QP search engine
- Ease-of-use: No command line interface necessary with GUI
- Interoperability with their current security system

Interoperability

Because of how the Quantea solution is designed, it works on any network and the end user can use any packet analysis tool they choose to read and analyze the captured and stored data. Such tools include Wireshark®, Splunk®, Cascade®, or any other tool. Plus, the system can integrate with any TAP, IDS/IPS, or Security solution and network monitoring system via simple APIs. *TAPs do not require APIs.