TCPWave IPAM

Domain Name System

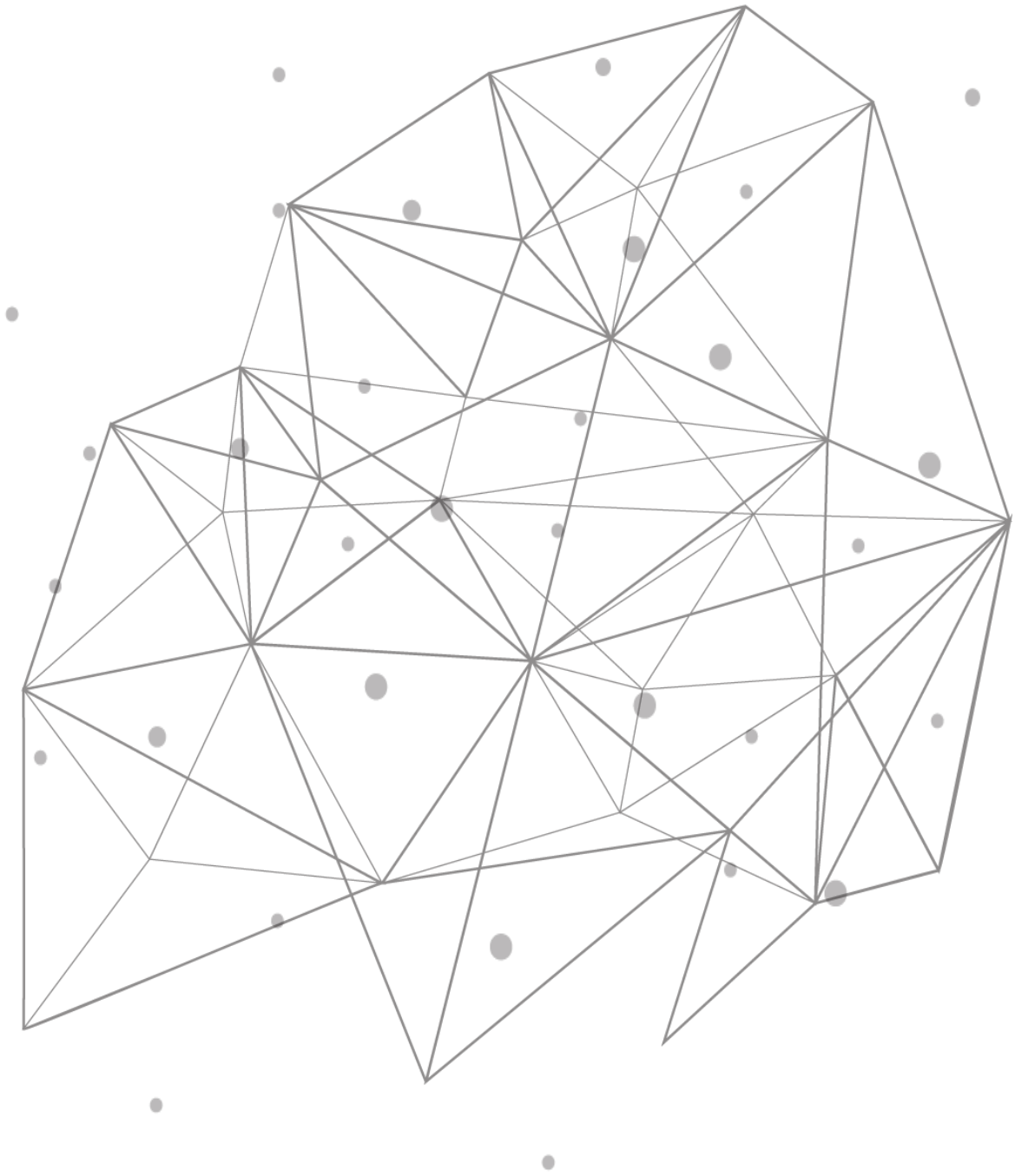


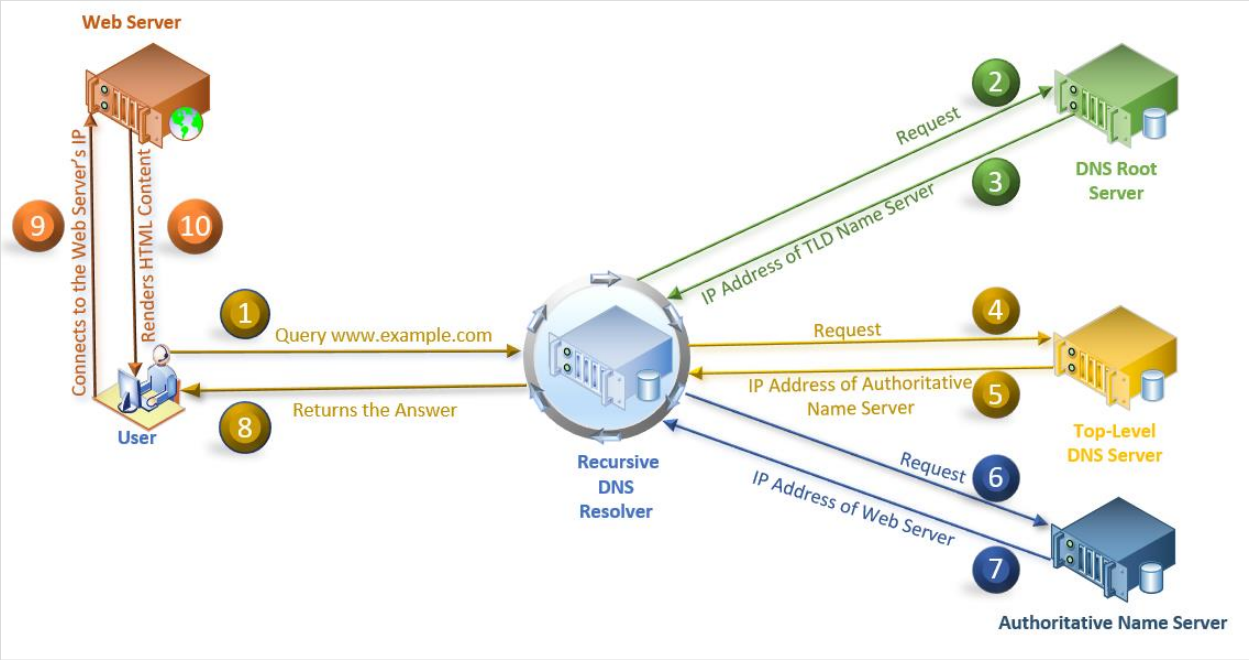
Table of Contents

Introduction

In the dynamic internet world era, all the applications that provide communication between devices use IP addresses to identify the communicating hosts. However, IP addresses are challenging for human users to remember, so humans utilize the name of the network interface as a substitute for an IP address. The relationship between the name of a network interface and an IP address is defined in the Domain Name System (DNS) database, distributed worldwide. So it is considered as one of the vital and fundamental components of today's modern networking world as it delivers the naming services for internet users, translating human-readable domains to numerical Internet Protocol (IP) addresses.

How DNS Works

DNS aims to resolve a fully qualified domain name (FQDN) to an IP address. This process is called name resolution, that is, query or response protocol. The client queries information, and DNS uses UDP Port 53 to connect to the server. When your computer wants to find the IP address associated with a domain name, it first requests a recursive DNS server, also known as a recursive DNS resolver. It is a server usually operated by an Internet Service Provider (ISP) or other third-party providers. It knows which other DNS servers it needs to query to resolve the name of a site with its IP address, as explained in the following diagram:



DNS Servers

Servers that work together to deliver the IP address of the requested website to the web browser are known as DNS Servers.

There are four types of DNS Servers:

- DNS Recursive Server (or) DNS Resolver
- Root Name Server
- Top-Level Domain (or) TLD Name Server
- Authoritative Name Server

Recursive DNS Resolver

All domains are allocated a unique IP address. When you type example.com, the browser response is to convert the URL into the IP address. The web browser initiates the process by utilizing an internal cache of recent DNS query results. The cache is the first place the browser checks to obtain the IP address of the domain. If this does not fetch in a DNS resolution, a client-side DNS resolver directs the query to a recursive DNS server that could exist at an Internet Service Provider (ISP).

Root Name Server

It gets involved when the DNS resolver does not find what it needs in its cache. There are 13 sets of root zone servers, which different organizations run. The 13 servers respond to the resolver with the IP address for the TLD name server.
Please refer to root servers for the URL details of all the root name servers.

TLD Name Server

Next, the request goes through the Top-Level Domain (TLD) name server. It stores the information of all domains sharing common domain extensions(.com, .in, .net, .edu).
Example: .com TLD name server stores the information of the websites ending with .com extensions
.net TLD name server stores the information of the websites ending with .net extensions.
The TLD name server then points the recursive server to the authoritative name server IP address.

Authoritative Name Server

This is the last stop in the name server query. It resolves the hostname to the correct IP address, then sends it to the recursive cached. It's then returned to the client's browser to access the requested site via the IP address.

Common Threats to DNS Servers

The DNS remains under constant attack, and there seems to be no end in sight as threats grow increasingly sophisticated. Cybercriminals recognize the worth of DNS and may look for ways to abuse improperly secured DNS to compromise its integrity. For all the enterprises, DNS is their digital identity and a significant component of the security architecture. Some of the common threats to DNS servers are:

- DNS Spoofing
- Denial-of-service (DoS) and Distributed denial-of-service attacks (DDoS)
- Domain hijacking
- Distributed reflection denial-of-service (DRDoS) attacks
- DNS flood attacks
- DNS tunneling
- Random subdomain attacks
- NXDOMAIN attacks
- Phantom domain attacks

DNS Spoofing, DoS attacks, and DDoS attacks are the most common DNS attacks that are explained in the following sections:

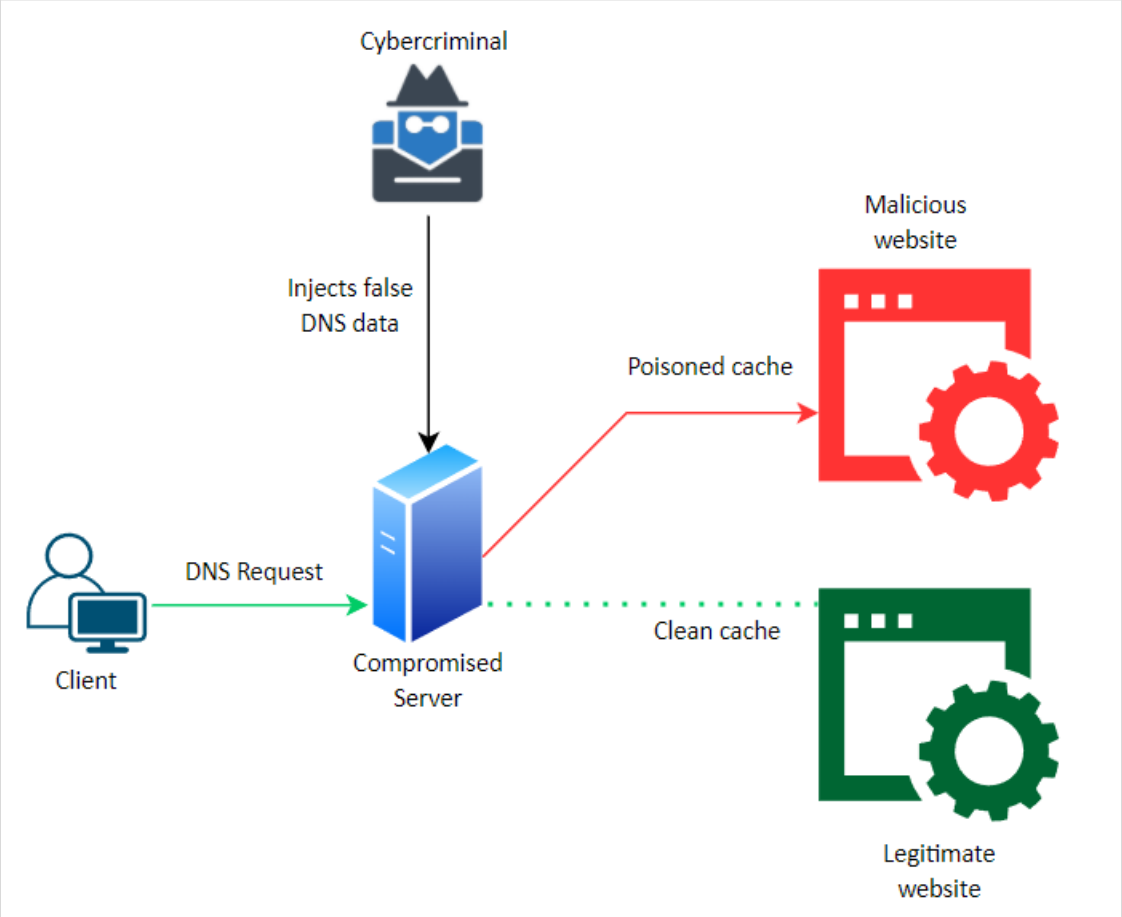
DNS Spoofing

DNS Spoofing is when the cybercriminals exploit the DNS to maliciously redirect the traffic with the intention of redirecting potential victims to fake content. The word "spoof" means to imitate or counterfeit, which the attack vector does. In most cases, cybercriminals use DNS spoofing for phishing attacks to get sensitive user credentials and login information from banks or payment services. It is done

by replacing the IP addresses stored in the DNS server with those under the cybercriminal's control. Once it is done, whenever the client tries to visit a particular website, they get directed to the malicious websites placed by the attacker in the spoofed DNS server. There are essentially two methods of DNS spoofing – DNS cache poisoning and DNS ID spoofing.

Cache Poisoning

It occurs when the local DNS server is replaced with the compromised DNS server. The compromised DNS server contains customized data entries of legitimate website names with the attacker's IP addresses. Hence, when a request is forwarded to the local DNS server for IP resolution, it communicates with the compromised DNS server, which results in the client being redirected to a deceptive website established by the attacker.



DNS ID Spoofing

In DNS ID spoofing, the packet ID and IP information produced for the resolve request sent by the client is duplicated with misleading details inside it. As the response ID matches the request ID, the client accepts the response containing the information that is not expected.

DoS and DDoS

These attacks entail one DoS or more than one DDoS source attacking the DNS and a website quickly. The aim is to cripple the infrastructure supporting the website by overwhelming it with excessive queries.

TCPWave Security Solutions

TCPWave security solutions help enterprises understand the network security vulnerabilities that threaten the enterprise's ecosystem. Furthermore, it prepares organizations for combating cyber-attacks proactively. TCPWave security features address the enterprise's needs and help streamline the security operations.

Conclusion

TCPWave's DDI solution helps our customers manage and modernize their enterprise-grade solutions by ensuring they have the most innovative technology with minimal risks.

For a quick demo, contact the TCPWave Sales Team.