**SPF**

SPF record is a DNS TXT Record, which mention that what mail servers are authorized to send mails on behalf of your domain. SPF record are introduced to stop spammers from sending messages with forged ‘From’ addresses of our domain.

TXT Record is used to implement the Sender Policy Framework (SPF) and DomainKeys specifications.

The technology requires two sides to work in tandem –

1. The domain owner publishes this information in an TXT Record in the domain's DNS zone, and when someone else's mail server receives a message claiming to come from that domain, then
2. The receiving server can check whether the message complies with the domain's stated policy. If, for example, the message comes from an unknown server, it can be considered a fake.

**DKIM**

"DKIM" stands for Domain Keys Identified Mail. DKIM creates a domain-level authentication framework for email, by using public-key technology and DNS record to prove the source and content of a message.

It’s a way to additionally sign your emails in a way that will allow the recipient’s server check if the sender was really you or not.

The main goal here is to someone from tampering with an email while in transit, DKIM provides an encryption key and digital signature that verifies that an email message was not faked or altered

The technology works like this,

DKIM automatically adds a digital signature to each message. This signature is based on a private key known only to your server. You then publish a public key in your domain’s DNS TXT record. The recipient server can then use the public key to decode the signature and be sure the message has not been altered

1. Private key - Which is unique to your domain and available exclusively to you. It allows you to encrypt your signature in the header of your messages.
2. Public key - Which you add to your DNS records using DKIM standard, in order to allow your recipient’s server, retrieve it and decrypt your hidden signature from the header of your message.

mail server (mail transfer/transport agent, MTA, mail router, Internet mailer)

A mail server is an application that receives mail from local users and remote senders, then forward that message for delivery.

A computer dedicated to running such applications is also called a mail server.

Common mail server programs - Microsoft Exchange, qmail, Exim and sendmail.

When an e-mail message is send, mail client/e-mail program, such as Outlook / Eudora / Thunderbird, forwards the message to your mail server, which in turn forwards it either to another mail server or to a holding area on the same server called a message store to be forwarded later. As a rule, the system uses SMTP (Simple Mail Transfer Protocol) or ESMTP (extended SMTP) for sending e-mail, and either POP3 (Post Office Protocol 3) or IMAP (Internet Message Access Protocol) for receiving e-mail.

MTA – Mail Transfer agent

IMAP – Internet Mail Access Protocol

POP – Post Office Protocol

**DNS Records**

**Address Record [A Record]**

Address (A) records is used to direct /point a hostname to a numerical IP address.

For example, if you want mycomputer.yourdomain.com to point to your home computer (which is, for example, 192.168.0.3), you would enter a record that looks like:

mycomputer.yourdomain.com. A 192.168.0.3

Important: You must put a period after the hostname, new cpanel works without period. Do not put periods after IP addresses.

**AAAA Records**

As IPv6 becomes more prevalent, the AAAA record (or "quad-A") will become more popular. This is simply the IPv6 equivalent of the IPv4 version, and it differs because IPv6 uses 128-bit addresses. This means that AAAA records are notated using eight groups of 16-bit values, such as: fe80:226:18ff:fed3::cc2a.

**Mail Exchanger [MX] Record**

MX records are those that are looked up by mail servers when email needs to be delivered, MX record specifies a mail exchange server for a DNS domain name. The information is used by Simple Mail Transfer Protocol (SMTP) to route emails to proper hosts. Typically, there are more than one mail exchange server for a DNS domain and each of them have set priority.

A MX Record has a Preference number indicating the order in which the mail server should be used (only relevant when multiple MX Records are defined for the same domain name). Mail servers will attempt to deliver mail to the server with the lowest preference number first, and if unsuccessful continue with the next lowest and so on.

A MX Record identifies the mail server(s) responsible for a domain name. When sending an e-mail to user@xyz.com, your mail server must first look up the MX Record for xyz.com to see which mail server actually handles mail for xyz.com (this could be mail.xyz.com - or someone else's mail server like mail.isp.com). Then it looks up the A Record for the mail server to connect to its IP-address.

**Canonical Name [Alias / CNAME] Record**

CNAME Records are domain name aliases, CNAME allows a machine to be known by one or more hostnames. There must always be an A record first, and this is known as the canonical or official name. For example:

A Record : domain.com. A 192.168.0.1

CNAME Record : ftp.domain.com. CNAME domain.com.

mail. domain.com. CNAME domain.com.

ssh. domain.com. CNAME domain.com.

CNAME records make it possible to access your domain through ftp.domain.com, mail.domain.com, etc. Without a proper CNAME record, you will not be able to connect to your server using such addresses.

The most popular use of the CNAME Record type, is to provide access to a Web Server using both the standard www.domain.com and domain.com (without the www). This is usually done by adding a CNAME-record for the www name pointing to the short name [while creating an A Record for the short name (without www)].

Sometimes companies register their multiple domain names for their brand-names but still wish to maintain a single website. In such cases, a CNAME Record maybe used to forward traffic to their actual website. For example, www.abc.in could be CNAMEd to www.abc.com.

**Authoritative Name Server [NS] Record**

NS Records identify DNS servers responsible (authoritative) for a Zone. A Zone should contain one NS Record for each of its own DNS servers (primary and secondaries). This mostly is used for Zone Transfer purposes (notify). These NS Records have the same name as the Zone in which they are located.

But the most important function of the NS Record is Delegation. Delegation means that part of a domain is delegated to other DNS servers.

You can also delegate sub-domains of your own domain name (such as subdomain.yourname.com) to other DNS servers. An NS Record identifies the name of a DNS server, not the IP Address. Because of this, it is important that an A Record for the referenced DNS server exists, otherwise there may not be any way to find that DNS server and communicate with it.

If a NS Record delegates a sub-domain (subdomain.yourname.com) to a DNS Server with a name in that sub-domain (ns1.subdomain.yourname.com), an A Record for that server (ns1.subdomain.yourname.com) must exist in the Parent Zone (yourname.com). This A Record is referred to as a Glue Record, because it doesn't really belong in the Parent Zone, but is necessary to locate the DNS Server for the delegated sub-domain.

**Text [TXT] Record**

A Text Record provides the ability to associate some text with a domain or a subdomain. This text is meant to strictly provide information and has no functionality as such. A TXT Record can store upto 255 characters of free form text. This record is generally used to convey information about the zone. Multiple TXT records are permitted but their order is not necessarily retained.

For example, you may add a TXT Record for yourname.com with the value as "This is my mail server". Here if anybody was checking ALL or TXT records of yourname.com, they would notice the above text appearing in the TXT record.

TXT Record is also used to implement the Sender Policy Framework (SPF) and DomainKeys specifications.

**PTR records**

Pointer records (PTR) are used for reverse lookups. For example, to make 192.168.0.1 resolve to www.yourdomain.com, the record would look like:

1.0.168.192.in-addr.arpa PTR www.yourdomain.com.

Note: The IP address is reversed in the first field. Please use a period after your hostname (second field).

The in-addr-arpa method is the most frequently used.

Important: PTR records are effective only if your site has its own IP address.

**Start of Authority [SOA] Parameters**

Each Zone contains one SOA Record, which holds the following parameters for the Zone -

**Name of Primary DNS Server** - The domain name of the Primary DNS Server for the Zone. The Zone should contain a matching NS Record.

**Mailbox of the Responsible Person** - The email address of the person responsible for maintenance of the Zone.

**Serial Number -** Used by Secondary DNS Servers to check if the Zone has changed. If the Serial Number is higher than what the Secondary Server has, a Zone Transfer will be initiated. This number is automatically increased by our Servers when changes to the Zone or its Records are made.

**Retry Interval** - How often Secondary DNS Server should retry checking, if changes are made - if the first refresh fails.

**Expire Interval** - How long the Zone will be valid after a refresh. Secondary Servers will discard the Zone if no refresh could be made within this interval.

**Minimum (Default) TTL** - Used as the default TTL for new records created within the zone. Also used by other DNS Server to cache negative responses (such as record does not exist, etc.).

**CloudFlare**

If your site or application users are distributed across different locations and cause load in origin server you should consider using a CDN to provide a pleasant user experience as it allows to deliver content fast and reliable and decrease load on the origin server so you don’t need to scale your own infrastructure.

CloudFlare is designed to accelerate (quick loading time) and secure any website. This system works somewhat like a content delivery network (CDN), that is to host your website static contents (A Static content is that which does not change much often like your website images, CSS, scripts. What CloudFlare does is that it downloads all your website static content to its server and from there it serves it to your website visitors) in its server and this static content is then served to your website visitors. It acts as a reverse proxy, a middleman between you—the user—and a given website. When you go to visit that site, you’ll be directed to one of Cloudflare’s servers instead of the actual site’s servers.

CloudFlare is a distributed network consisting of 79 Data Center worldwide. These Data Center are located in all major countries like USA, UK, India, Russia, Japan, China, South Africa, Australia, Brazil and many more. All these Data Center contains your website static content.

Now whenever a person visits your website, CloudFlare detects the physical location of that person, then it directs the Data Center nearest to the user (in Geographic term) to serve the static content. This makes the process quick and greatly increases the performance and loading speed of your website.

CloudFlare add security to your website. You have to change your Nameservers in DNS to that provided by CloudFlare. That means CloudFlare knows everything about your website traffic.

It is right to say that CloudFlare acts as a Protective Shield, hiding your website from direct access.It also known what type of visitors are coming in your website. It can detect spammers, brute force request, etc. I would say its security algorithm is quite smart to detect all such things. CloudFlare protects against a range of threats: cross site scripting, SQL injection, comment spam, excessive bot crawling, email harvesters, and more.

Advantages :

Cloudflare to ensure you’re a legitimate user (thus protecting against denial of service attacks), load the site faster (since they’ve cached certain parts of the site), and protect against downtime (since they have multiple servers worldwide and can fall back on any server if one has a problem).

CDN (Content Delivery Network): It delivers content from the location closest to the visitor. This speeds up your site’s loading time.